Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Cláudia da Silva Mendonça

GUERRA CIBERNÉTICA:
Desafios de uma Nova Fronteira

Rio de Janeiro

2014

Cláudia da Silva Mendonça

GUERRA CIBENÉTICA:

Desafios de uma Nova Fronteira

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Claudio Miceli de Farias, M.Sc., UFRJ, Brasil

Rio de Janeiro

2014

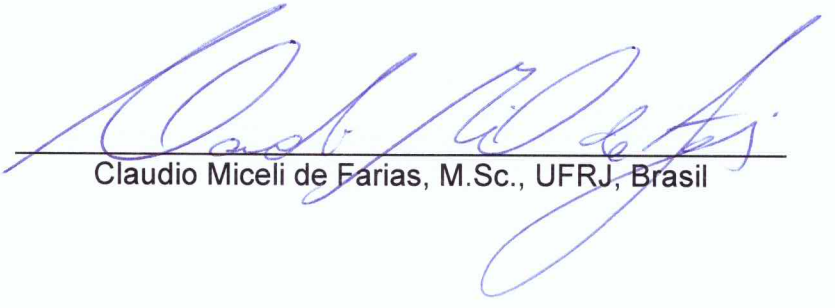
Cláudia da Silva Mendonça

GUERRA CIBERNÉTICA:

Desafios de uma Nova Fronteira

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2014.



Claudio Miceli de Farias, M.Sc., UFRJ, Brasil

AGRADECIMENTOS

A Deus que mostrou Seu fôlego de vida em mim, me sustentou e me deu coragem para questionar a realidade e propor sempre um novo mundo de possibilidades... Sem a ajuda Dele eu não sou nada.

A minha mãe Helle-nice e meu esposo Roberto que acreditaram em mim, me deram a esperança para seguir em frente, apesar das dificuldades, a segurança e certeza de que não estou sozinha nesta caminhada. Só vocês entendem o meu objetivo, falta de tempo, o cansaço, a necessidade de isolamento que a escrita exige. Obrigada pelo apoio neste momento tão difícil.

Ao Professor e orientador Claudio Miceli de Farias pelo seu apoio e inspiração no amadurecimento dos meus conhecimentos e conceitos que me levaram à conclusão desta monografia.

Aos amigos e professores Alexandre Ramos e Marcelo Ribeiro que me despertaram o desejo de trilhar este caminho e me mostraram alguns pontos de pesquisa.

A minha amiga Roberta pela sua amizade e companheirismo em todos estes anos, pelos seus inúmeros conselhos e pelas palavras de estímulos, que muito me ajudaram a continuar a caminhada.

Aos colegas de especialização pela oportunidade de convívio e, em especial, ao amigo de turma Sergio Machado que, com muita paciência e atenção, dedicou um pedaço do seu tempo para me apoiar e incentivar durante todo o curso, tanto nesta pesquisa quanto no nosso cotidiano de aulas presenciais.

Aos meus companheiros de trabalho que contribuíram para que eu pudesse subir mais este degrau. Vocês são os profissionais que me inspiram diariamente.

RESUMO

MENDONÇA, Cláudia da Silva. **GUERRA CIBERNÉTICA: Desafios de uma Nova Fronteira**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

Com o avanço da tecnologia da informação e comunicações (TIC) aliado ao aumento de acessos à Internet e redes sociais, o grande desafio da Era Digital é a construção de um ambiente no País que permita identificar, monitorar e mitigar os riscos cibernéticos, impulsionando o desenvolvimento de ações preventivas, pró-ativas, reativas e de repressão a todo o tipo de ameaça, a fim de assegurar e defender os interesses do país e da sociedade brasileira.

Os tipos de ataques de negação de serviço, as tentativas de interceptação de trafego e a engenharia social, são algumas armas que estes cibercriminosos possuem e do outro lado desta guerra, temos algumas ferramentas e equipamentos que nos auxiliam na proteção da rede.

Este trabalho de conclusão de curso apresenta alguns ataques ocorridos no mundo que deram início a era cibernética, algumas técnicas de ataque e ferramentas de defesa, bem como propõe uma solução de defesa para proteger as infraestruturas críticas do País e das organizações.

Palavra-chave: Guerra Cibernética.

ABSTRACT

MENDONÇA, Cláudia da Silva. **GUERRA CIBERNÉTICA: Desafios de uma Nova Fronteira**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

The advancement of Information and Communication along with increased access to the Internet and social networks, the challenge of the digital age is to build an environment that allows the country to identify, monitor and mitigate cyber risks, boosting the development of preventive, proactive, reactive and repressive actions to any kind of threat, in order to secure and defend the interests of the country and the Brazilian society.

The types of denial of service attacks, intrusion attempts and social engineering are the weapons that these cybercriminals have and the other side of this war, we have some tools and equipment that assist us in protecting the network.

This course conclusion work presents some attacks in the world who started the cyber age some techniques of attack and defense tools, and proposes a solution of defense to protect the critical infrastructure of the country and organizations.

Keyword: CyberWar.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ACK	*Acknowledge*
AP	*Access Point*
APF	Administração Publica Federal
ARP	*Address Resolution Protocol*
CLP	Controlador Lógico Programável
DDoS	*Distributed Denial of Service*
DLP	*Data Loss Prevention*
DNS	*Domain Name System*
DoS	*Denial of Service*
DRDoS	*Distributed Reflection Denial of Service*
ESSID	*Extended Service Set Identification*
FFAA	Forças Armadas
FTP	*File Transfer Protocol*
GC	Guerra Cibernética
HD	*Hard Disk*
HIDS	*Host-based Intrusion Detection system*
HPPTS	*Hypertext Transfer Protocol Secure*
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
IPS	*Intrusion Prevention Systems*
IPSEC	*IP Security Protocol*
MAC	*Media Access Control*
MITM	*Man-in-the-Middle*
MSVC	*Microsoft Visual Studio Compiler*
NIDS	*Network Intrusion Detection System*
OO	*Object Oriented*
POP	*Post Office Protocol*
SI	Segurança da Informação
SID	Segurança das Informações Digitais
SIEM	*Security Information and Event Management*
SMTP	*Simple Mail Transfer Protocol*
SQL	*Structured Query Language*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SYN	*Synchronize*
TCP	*Transmission Control Protocol*
TFN	*Tribe Floof Network*
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e Comunicação
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*
WAF	*Web Application Firewall*

SUMÁRIO

1 INTRODUÇÃO

Com a necessidade crescente de gerenciamento da informação distribuída em pontos fisicamente diferentes movido por uma economia altamente competitiva e instável, surgiu a Era da Tecnologia da Informação (TI) [1].

Novas tecnologias e métodos para se comunicar surgiram no contexto da Revolução Informacional e foram desenvolvidas gradativamente nos anos 90. Estas tecnologias utilizam a digitalização e a comunicação em redes para a transmissão e distribuição das informações. O advento da TI possibilitou o surgimento do que se pode chamar de "sociedade da informação".

A partir daí, a TI se transformou em base de todos os ramos do conhecimento, criando uma dependência cada vez maior. Porém, além dos inúmeros serviços prestados, as vulnerabilidades[2] são proporcionais a sua grandiosidade, sendo muitas vezes exploradas por pessoas mal intencionadas, que buscam vantagens com a exploração da falta de regras e são acobertadas pela distância e pelo aparente anonimato.

Logo se percebeu a possibilidade de explorar os recursos e as vulnerabilidades da TI sobre as infraestruturas críticas de um Estado, a fim de se obter informações confidenciais, realizar sabotagens ou mesmo ter vantagem durante a ocorrência de conflitos, independentemente dos atores envolvidos. Esta exploração das vulnerabilidades pode ser realizada por individuo, grupo ou por um Estado, sendo chamados de ataques cibernéticos ou guerra cibernética (GC).

A guerra na era da globalização mudou em sua lógica, apresentando-se com um novo formato. As mudanças não foram nos instrumentos da guerra, na

[1] TI (Tecnologia da Informação) – É o conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir a produção, armazenamento, transmissão, acesso e o uso das informações. (ALECRIM, 2011).

[2] Vulnerabilidade - Qualquer ponto fraco, processo ou ato administrativo ou exposição física que torne um computador suscetível à exploração por uma ameaça (MICROSFT, 2006)

tecnologia dos meios empregados no seu planejamento e execução, nos modelos de condução da guerra ou nos tipos de guerra e sim na natureza da guerra, suas funções e eficiência de suas ações.

Atualmente, ser o maior em poder bélico e grande quantidade de combatentes já não é garantia de inviolabilidade, pois não sabemos onde está o inimigo, uma vez que a internet não tem fronteira física.

A combinação de velhos valores e novas tecnologias gera desconforto, desconfiança e desacordo entre os países, então os ataques cibernéticos se apresentam em uma escalada mundial crescente, silenciosa e se caracterizam como um dos grandes desafios do século XXI. Todas as pessoas, empresas, governos e entidades que utilizam o espaço cibernético estão expostos a riscos.

Com o aumento da independência dos sistemas digitais aliado à conectividade global, a informação passa a ser um ativo crucial para os países administrarem sua segurança nacional e coletiva, objeto permanente da atenção das forças armadas e governo.

1.1 MOTIVAÇÃO

Os desafios de uma nova modalidade de guerra, o conhecimento de novos conceitos e o desejo de fazer desta pesquisa um ponto inicial para estudos mais detalhados e, assim, a oportunidade de novos debates e possível crescimento do País neste setor foram alguns dos motivos que contribuíram para que houvesse uma persistência neste tema de pesquisa.

1.2 RELEVÂNCIA

A GC por ser assimétrica, barata e altamente destrutiva, faz com que povos mais fracos consigam entrar em conflito com grandes potências e lutar em igualdade, o que não acontecia nas guerras tradicionais do passado.

Atualmente, sabemos que nenhuma nação está completamente protegida contra ataques virtuais, sendo necessário que o atacante seja patrocinado por uma estatal e tenha motivações políticas intrínsecas para realizar tais ataques, o que necessitaria de uma estrutura e estratégia de guerra clássica.

Diante do aumento dos ataques envolvendo conflitos entre países, há a necessidade um estudo mais detalhado, então este trabalho analisa os pontos importantes de algumas técnicas e ferramentas de ataque e defesa, que podem mostrar a superioridade ou fragilidade do Pais diante desta tão potente guerra virtual, a qual utiliza o ciberespaço como Teatro das operações para enfraquecer e causar caus ao inimigo.

1.3 RESULTADOS ESPERADOS

O Brasil atualmente está iniciando nesta área e possui uma postura defensiva sobre este tema, possuindo somente ações para prevenir o ataque, então é necessário uma evolução desta postura, a fim de nos prepararmos para retribuir tais ofensivas, e a conscientização da sociedade, os treinamentos e as simulações são pontos primordiais para este crescimento.

Da mesma forma, com este estudo esperamos alcançar uma maior especialização nacional nesta área, a fim de podermos ter uma postura pró-ativa, avaliando as vulnerabilidades e potenciais ameaças às estruturas críticas do País.

1.4 OBJETIVO

O trabalho tem como objetivo analisar os desafios deste novo paradigma de guerra, apresentar métodos e técnicas de ataque, ferramentas de defesa, vulnerabilidades que representam potenciais ameaças e os impactos das dinâmicas da Guerra Cibernética na sociedade da informação, focando nas perspectivas das Forças Armadas.

1.5 ORGANIZAÇÃO

O trabalho está organizado da seguinte forma:

- No capítulo 2 é apresentada uma breve explanação sobre conceitos clássicos de guerra e alguns conceitos usados em segurança Cibernética, princípios e GC e principais ataques cibernéticos ocorridos nos últimos anos.
- No capítulo 3 será elucidado sobre os métodos, técnicas e ferramentas de ataques mais comuns e as vulnerabilidades exploradas.
- No capitulo 4 será mostrado as ferramentas de defesa mais utilizadas em ataque.
- No capitulo 5 será proposto uma abordagem integrada como melhor forma de proteção dos ataques cibernéticos.
- Por fim, serão apresentadas na conclusão as medidas a serem adotadas pelo País para se proteger de ataques e para minimizar seus efeitos e o que esperar do futuro nesta área.

2 ASPECTOS GERAIS SOBRE GUERRA CIBERNÉTICA

A constante evolução tecnológica ocorrida nos últimos anos resultou em grandes benefícios para a Sociedade, porém, trouxe problemas relacionados à segurança da informação digital[3] (SID) que são frutos dessa própria evolução tecnológica, a qual possibilitou a integração cada vez maior de ambientes e de redes diferentes.

Com esta evolução crescente, ameaças também surgiram para explorar estas novas descobertas e a segurança da informação (SI) deve estar muito bem implementada e massificada na mente dos usuários e profissionais de TI, a fim de evitar a ocorrência de incidentes que possam afetar a todos.

A TI cria a necessidade do Estado adaptar suas estratégias de emprego da força a esta nova ferramenta. A informação é um bem público a ser protegido e controlado, servindo como uma arma na luta por territórios, por credibilidade e na guerra de ideias (MANJIKIAN, 2010).

Com esta evolução, alguns termos são relativamente novos e passaram a fazer parte da rotina dos profissionais da área de TI nas esferas empresariais e governamentais. Estes conceitos têm sido muito discutidos e estudados por especialistas e vem levantando a necessidade de preocupação com os seus impactos, então antes de evoluir no pensamento sobre estes termos, é necessário certificar-se do que cada um deles representa.

2.1 GUERRA DA INFORMAÇÃO

O avanço da tecnologia proporcionou novas formas de se comunicar, ao mesmo tempo em que trouxe dependências e vulnerabilidades às organizações e

[3] Segurança da Informação digital (SID) – É a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO 27002, 2005).

com isso surgiu a disputa pelo recurso da informação, a qual deve ser administrada de forma diferenciada, servindo de recurso essencial estratégico de um governo ou organização.

Na ultima década, o controle da informação está substituindo a segurança nacional como prioridade estratégica das grandes potências. Esta é uma mudança significativa no mundo atual, mostrando o papel que a informação passou a ter não só no dia a dia das pessoas, mas como estratégia política de uma nação (CASTILHO, 2013).

Com a evolução da tecnologia da informação há a necessidade do Estado adaptar suas estratégias, uma vez que a informação é o bem a ser controlado e serve de arma a favor do domínio por um território, por atendimento de interesses nacionais, pelo poder e por credibilidade. As nações utilizam diferentes estratégias virtuais para alcançar os mesmos objetivos reais, unindo a guerra virtual à guerra real, a fim de desmobilizar o inimigo.

A mídia vem noticiando constantemente os termos “Guerra da Informação”, “Guerra Eletrônica”, “Guerra Cibernética” e “Guerra Assimétrica” como sinônimos e percebemos a falta de consenso entre estudiosos na definição destes termos, mas podemos definir Guerra da Informação, como um conflito onde o alvo é a informação (SCHWARTAU,1994).

E Guerra Cibernética é um subconjunto da guerra da informação, que envolve ações realizadas na Internet e nas redes a ela relacionadas (PARKS; DUGGAN,2001).

Já a Guerra Eletrônica é entendida como ações que visam o controle e domínio do espectro eletromagnético para impedir, reduzir ou prevenir seu uso contra os interesses do país (BRASIL, 1999).

A Guerra da Informação tem o objetivo de alcançar a superioridade informacional frente ao oponente (WU, 2006), num contexto de competição ou operação militar, onde terá melhores condições para vencer aquele que conseguir se antecipar à execução dos ataques[4] e, assim, reagir ofensivamente com a maior rapidez possível. Para isso, é necessário ter ferramentas de monitoramento e pessoal qualificado para rastrear possíveis ataques.

Existem conceitos básicos que estão sendo delineados pelos especialistas da área de Segurança da informação e concordam que os atributos disponibilidade, integridade, confidencialidade são os principais e que melhor definem as propriedades da SI (KRAUSE, 1999), porém o Comitê Gestor de Segurança da Informação (CGSI)[5], entende que o atributo autenticidade tem a mesma importância que os termos supracitados.

Apesar de reconhecer que outros autores trabalham com outros atributos, KRAUSE (1999) prefere manter o foco nesses três princípios básicos para garantir a SI:

> • Confidencialidade. A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.
>
> • Disponibilidade. A informação deve estar disponível no momento em que a mesma for necessária.
> • Integridade. A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas.

[4] Ataque é o conjunto de ações que tentem comprometer a integridade, confiabilidade ou disponibilidade de um recurso computacional (BOFF, 2009).

[5] Comitê Gestor de Segurança da Informação (CGSI) - Comitê que assessora a Secretaria Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos no Decreto Nº 3505 de 13 de junho de 2000.

2.2 ESPAÇO CIBERNÉTICO

O mundo cibernético (*Cyber War*) é qualquer realidade virtual [6], numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a *Internet* e as redes a ela relacionadas, as quais compartilham mídia com a Internet (PARKS; DUGGAN, 2001).

Para estes autores, o mundo cibernético é uma realidade virtual que se contrapõe à guerra cinética, definida como a guerra praticada no mundo real.

É muito difícil falarmos em fronteiras físicas no espaço cibernético (ciberespaço), uma vez que não temos como definir os seus limites e a soberania de cada Estado, juntamente com a dificuldade em definirmos a identidade das pessoas que se apresentam por seus apelidos (*nicknames*) e nem delinearmos suas ações. Desta forma, o ciberespaço é um não-lugar: sem fronteiras, sem raízes, sem história (AUGE, 1994).

Diante disso, como identificarmos a fronteiras do espaço cibernético? A questão desta nova fronteira encontra-se no limbo jurídico, não está perfeitamente demarcada e sem regras bem definidas, o que impossibilita o Estado de aplicar a lei, havendo a necessidade eminente de um estudo detalhado sobre este assunto, a fim de definir as fronteiras do ciberespaço e as responsabilidades de cada nação.

2.3 GUERRA CIBERNÉTICA

É uma nova modalidade de guerra que vem assustando a todo o mundo, onde o ciberespaço e tecnologias de informação são o cenário principal em vez do campo

[6] Realidade Virtual – Este termo foi creditado à Jaron Lanier, fundador da VPL *Research* Inc., que o cunhou, no início dos anos 80, para diferenciar as simulações tradicionais feitas por computador de simulações envolvendo múltiplos usuários em um ambiente compartilhado (ARAÚJO, 1996).

de batalha convencional e os conflitos não possuem armas físicas, mas o confronto é realizado com meio eletrônicos no mundo virtual.

Devido a este tipo de guerra ser muito atual, então este assunto possui várias definições em várias obras diferentes, entretanto, neste trabalho, será considerado o conceito apresentado no Manual MD35-G-01, (BRASIL, 2007):

> Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de comunicações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (BRASIL, 2007).

Apesar de não haver um acordo na definição deste tema, um aspecto que todos os autores concordam é que para ocorrer a GC é necessária a existência de motivação estratégica ou política realizada por ou contra um País, então atividades realizadas com motivações pessoais não podem ser consideradas como sendo GC, embora possam ser igualmente prejudiciais.

Na visão do Ministério da Defesa (MD), conforme o definido no Manual MD30-M-01 das Forças Armadas (BRASIL, 2011), a GC é composta das seguintes ações:

> • Exploração Cibernética – consiste em ações de busca, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados, de forma não autorizada, para a produção de conhecimento e/ou identificar as vulnerabilidades desses sistemas (BRASIL, 2011).
>
> • Ataque Cibernético – compreende ações para interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos e redes computacionais e de comunicações do oponente (BRASIL, 2011).
>
> • Proteção Cibernética – abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança Cibernética em face de uma situação de crise ou conflito armado. (BRASIL, 2011).

As ações de exploração e ataque cibernéticos são realizadas em conjunto, a fim de ter o controle da Infraestrutura Criticas de informações[7], obter dados sigilosos e indisponibilizar todos os sistemas indispensáveis do inimigo e, com isso, acabar com o poder do inimigo. Já as ações defensivas de proteção cibernética empregará procedimentos e dispositivos para se contrapor às táticas que podem ser empregadas pelo oponente.

2.4 PRINCÍPIOS DA GUERRA CIBERNÉTICA

A partir do trabalho inicial de PARKS e DUGGAN, apresentado no Seminário de SI da Academia Militar dos Estados Unidos da América (USMA) [8], em 2001, foi verificado que alguns princípios da Guerra Tradicional não se aplicavam ao mundo virtual, sendo necessário propor novos princípios em um estudo posterior (CAHILL; ROZINOV; MULÉNUM, 2003):

- O ataque cibernético [9] só faz sentido se produzir algum efeito no mundo real e com isso obter algumas vantagens por meio das suas ações realizadas;
- Todo ato feito no mundo virtual é visível, mesmo que medidas para dissimular sejam realizadas;
- No mundo virtual não possível prever com exatidão o comportamento resultante de uma ação tomada, devido à natureza imprevisível da operação de equipamentos e programas, exceto aquelas que refletem uma ação tomada no mundo físico;

---

[7] Infraestrutura Critica de Informações – É o subconjunto dos ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (MANDARINO, 2010).

[8] *United States Military Academy* (USMA) – É conhecida também como Academia de West Point, ou simplesmente pela sua sigla em inglês, USMA, é uma Academia Federal de Educação Militar de 4 anos, do Exército dos Estados Unidos, localizada em West Point, Nova Iorque.

[9] Ataque Cibernético - Compreende ações para interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos e redes computacionais e de comunicações do oponente (EB, 2013).

- O atacante pode assumir a identidade de outra pessoa para realizar atividades no mundo cibernético;
- As ferramentas de GC podem servir tanto para o ataque quanto para a defesa;
- O mundo virtual não é confiável. Os equipamentos e programas nem sempre produzem resultado da forma que esperamos, impossibilitando a certeza de que a próxima ação cibernética irá funcionar;
- Não existe distância física no mundo cibernético e esta não é obstáculo na condução de um ataque, então ações realizadas em diferentes localidades terão a mesma eficiência, dificultando a detecção da origem de ataques; e
- Quem controlar a parte do ciberespaço que o oponente utiliza, pode controlar o oponente (PARKS e DUGGAN, 2001).

2.5 ATAQUES CIBERNÉTICOS

Tem sido noticiado na mídia o crescimento de 42% dos ataques direcionados à espionagem industrial, no ano de 2012, incluindo a descoberta de 14 vulnerabilidades *zero-day*[10] e o aumento de 30% dos ataques *Web*, conforme revelou o Relatório de Ameaças à Segurança na Internet (ISTR) (SYMANTEC, 2012).

O relatório mostrou que os cibercriminosos não estão reduzindo suas atividades e continuam a planejar novas maneiras de roubar informações de organizações de todos os tamanhos. As sofisticações dos ataques combinadas com a atual complexidade da TI exigem que as empresas se mantenham pró-ativas e

[10] Vulnerabilidade *Zero-Day* – É aquela reportada por ter sido explorada em seu estado selvagem, antes da vulnerabilidade ser de conhecimento público e de ter uma atualização disponível (SYMANTEC, 2012).

usem medidas de segurança com defesa avançada para prevenir ataques, afirmou André Carrareto, Estrategista em Segurança da Symantec para o Brasil.

Figura 1 – Total de incidentes reportados ao CERT.br no período de JUL a SET2013. Fonte: CERT.BR, 2013a.

O limiar para se definir ataque cibernético e guerra no ciberespaço é muito tênue (LEWIS, 2010). Para ele, guerra cibernética deve ser entendida como o uso da força, pelos Estados ou grupos políticos, para causar destruição, danos ou vítimas de efeito político ou estratégico. Estas ações atingem as infraestruturas críticas de informações de um País, sendo decisiva e por si só gerar a vitória no combate.

Enquanto que um ataque cibernético é uma ação realizada por um indivíduo ou grupo individual com o intuito de provocar danos (físicos, financeiros ou morais), destruição ou vítimas sem que tenham o objetivo de obter uma vantagem estratégica.

2.5.1 Caso Estonia

O ataque feito contra a Estônia mostrou na realidade a capacidade que tem um ataque cibernético (CLARK e KNAKE, 2010), protagonizando a primeira guerra virtual e sendo um divisor de águas em termos da ampla conscientização acerca da vulnerabilidade da sociedade moderna.

A Estonia é um país que tem sua infraestrutura totalmente informatizada, os serviços essenciais são virtualizados.

Após a retirada de uma estátua de bronze em Abril de 2007, a qual comemorava os soldados do Exército Vermelho que combateram os nazistas na Segunda Guerra Mundial, estourou o estopim da, até então conhecida, primeira GC (essa data ficou conhecida posteriormente como "*The Night Bronze*") (SHEETER, 2007).

O Governo estoniano disse ao site BBC[11] que seus sites e muitos sites de empresas e bancos do país estão sendo bombardeados por uma enorme quantidade de pedidos de informação, acima da capacidade de processamento dos seus servidores, obstruindo os servidores e roteadores, com isso os serviços essenciais saíram do ar, deixando aquele pequeno país completamente desconectado.

A fim de ampliar o ataque, os *hackers*[12] infiltraram computadores em todo o mundo com softwares, conhecidos como *botnets*[13]*,* para realizar os ataques coordenados.

A partir desse fato, fica evidenciado que um ataque de negação de serviço

---

[11] Conforme noticiado no site da BBC, disponível em http://www.bbc.co.uk/portuguese /reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml.

[12] *Hacker* – É o indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos, a partir de uma conexão remota em uma rede de computadores. (FERREIRA, 1999).

[13] *Botnets* - É uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots (CERT.BR, 2013b).

distribuído (DDoS - *Distributed Denial of Service*)[14] bem sucedido pode não comprometer a infraestrutura física de um País, mas certamente causa danos e prejuízos, além do efeito psicológico. Com isso, o País perdeu sua força de ataque sem que nenhuma vida humana se perdesse pelo motivo do ataque cibernético.

2.5.2 Caso Stuxnet

Em Junho de 2010, foi descoberto o *malware*[15] chamado STUXNET, o qual marcou o início da década do terrorismo cibernético, com armas e guerras virtuais, sendo projetado para danificar fisicamente os equipamentos de controle industrial do Irã.

O Stuxnet foi desenvolvido para atacar somente em sistemas operacionais SCADA feita pela empresa Siemens (MCMILLAN, 2010). Este engenho norte-americano / israelense foi desenhado para retardar o avanço do programa nuclear iraniano.

O Stuxnet foi o primeiro *worm*[16] que tinha um *rootkit*[17] de CLP (Controlador Lógico Programável[18]), ou seja, ele tinha embutido comandos de baixo nível do sistema que tinha ação sobre o hardware, podendo reprogramá-lo sem que os funcionários notassem.

---

[14] *Distributed Denial of Service* (DDoS) - DDoS é o acrônimo de Distributed Denial of Service, um tipo de ataque em que um computador-alvo recebe uma quantidade tal de requisições que o sobrecarregam, tornando indisponíveis os serviços por ele oferecidos (OLIVEIRA, 2011).

[15] Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador (CERT.BR, 2013b).

[16] *Worm* - É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador (CERT.BR, 2013b).

[17] *Rootkit* - É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido (CERT.BR, 2013b).

[18] CLP (Controlador Lógico Programável) – São também computadores, mas altamente especializados para controle de infraestrutura industrial como atuadores e sensores industriais. Os CLPs rodam um sistema operacional próprio chamado SCADA (Supervisory Control and Data Aquisition) e não dependem diretamente de sistemas operacionais de PC. Foi aí que o Stuxnet provavelmente atuou, carregando no CLP códigos mal-intencionados (SILVA, 2011).

O *vírus*[19] conseguiu alterar a velocidade dos rotores das usinas nucleares e ao mesmo tempo enganava o sistema supervisor para que não detectasse qualquer anormalidade. Com isto, sem ser notado, superaquecia as plantas de produção até sua destruição. Quando se identificou que havia algo errado, os prejuízos estavam estabelecidos e o cenário era irreversível (FALLIERE; MURCHU; CHIEN, 2011).

Segundo o relatório do jornal americano *The New York Times*, publicado em Agosto de 2013, os analistas de segurança cibernética suspeitam que este supervírus fosse um esforço conjunto norte americano-israelense, apelidado de "*Olympic Games*" (SANGER, 2012).

Há muita especulação sobre a origem do Stuxnet. A Symantec e a Kaspersky concluíram que o seu desenvolvimento não poderia ter sido feito por usuários domésticos, mas somente pelo governo de algum país (FALLIERE; MURCHU; CHIEN, 2011). Constatou-se nas linhas de código do vírus que apresentavam registro de vários teclados do mundo, ou seja, ele pode ter sido desenvolvido em colaboração entre países, ou então isso foi feito apenas para cobrir rastros, não havendo ainda certeza sobre o que de fato ocorreu.

Hoje, todo o código fonte do Stuxnet está disponível na internet, e a preocupação é como ele poderá ser alterado de maneira a ser reutilizado. Existem indícios de que dois outros *vírus* são frutos dele, o Duqu e o Flame, ambos com foco no roubo de informações (FERRAN, 2012).

Esses eventos podem ser considerados como o início da primeira ciberguerra em escala global, o que deve ser visto não só por agências governamentais, mas por todos os profissionais responsáveis por sistemas críticos (SILVA, 2011a).

---

[19] *Vírus* – É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos (CERT.BR, 2013b).

2.5.3 Caso Duqu

Em 2011, os profissionais da área de Segurança das Informações Digitais e GC tomaram conhecimento desta nova arma cibernética, mas suspeitava-se que este novo *vírus* poderia estar ativo desde 2007, segundo relatos de analistas da Kaspersky Lab. Ele é uma variação do Stuxnet e teve um projeto sofisticado para roubar dados dos sistemas e depois atacá-los.

Os especialistas da Kaspersky verificaram que as vítimas eram infectadas por um *malware* introduzido através de um documento falsificado de Word, o qual, se aberto, desencadeia a instalação do Duqu.

Este código malicioso (*malware*) se aproveitava de um *zero-day* do Sistema Operacional Windows para se hospedar e então fazer a coleta das informações. Após extensas pesquisas do Laboratório da empresa de computação Russa Kaspersky, os cientistas entenderam que esse foi um software desenvolvido como um sucessor ou uma ferramenta adicional do Stuxnet para um ataque cibernético direcionado (KEIZER, 2011).

Até hoje não se sabe qual foi à linguagem de programação em que esse *worm* foi desenvolvido, nem seu desenvolvedor e o seu real motivo. Segundo COMPUTERWORLD (2012), os peritos anti-malware da Kaspersky Lab descobriram é que parte do programa parece ter sido desenvolvida com *Object Oriented* C (OO C), uma extensão arcaica personalizada para a linguagem de programação C. Enquanto a maior parte do Duqu foi escrito na linguagem C++ e compilado com o Microsoft Visual C++ 2008, o módulo de Comando foi escrito em C puro e compilado com Microsoft Visual Studio Compiler 2008 (MSVC 2008), usando duas opções específicas para manter o código pequeno.

Após uma extensa análise feita pela Empresa Symantec Labs, foi verificado

que parte do Duqu foi feita baseando-se em segmento do código-fonte do Stuxnet, deixando entendido que a pessoa ou organização que desenvolveu tenha tido acesso ao código-fonte integral da versão original, ou ao menos, fez parte de seu desenvolvimento (GALLAGHER, 2011).

A função do Duqu é roubar as senhas que são cruciais para a ação do Stuxnet, ou seja, o Duqu é um espião projetado para roubar informações das empresas que, provavelmente, seriam alvo da ação do Stuxnet.

2.5.4 Caso Flame

Em 2012, uma nova ameaça cibernética é noticiada pela mídia mundial, onde o Oriente Médio é mais uma vez alvo de ataques cibernéticos.

Inicialmente, o Flame não causava danos físicos aos computadores, pois ele foi projetado com intuito de roubar informações das máquinas infectadas, por meio da coleta de informações digitadas em campos de texto, gravação de áudio, captura de imagens e coleta de informações sobre aparelhos com Bluetooth desprotegido.

Segundo Gris (2012), a Kaspersky descreve como um *ataque toolkit*, o que significa que ele tem componentes suficientes para fazer qualquer, desde abrir um *backdoor* [20], implantar *trojans*[21] com várias finalidades e depois ir se espalhando como todo *worm*.

Pesquisadores da empresa também confirmaram que os autores dos vírus Flame e Stuxnet cooperaram em algum momento, uma vez que o Stuxnet utilizava um código idêntico a um *plugin* do vírus Flame, criando a ligação entre os dois vírus (ROHR, 2012).

---

[20] *Backdoor* – É um programa que *permite* o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim (CERT.BR, 2013b).

[21] *Torjan* (cavalo de tróia) – É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário (CERT.BR, 2013b).

A sofisticação, o número restrito de alvos e a ausência de um interesse comercial claro indicam que o Flame teria sido patrocinado por um governo, de acordo com os especialistas, e seria, portanto, uma arma de ciberespionagem (NEWMAN, 2012a). A figura 2 mostra a disseminação desta praga no mundo.

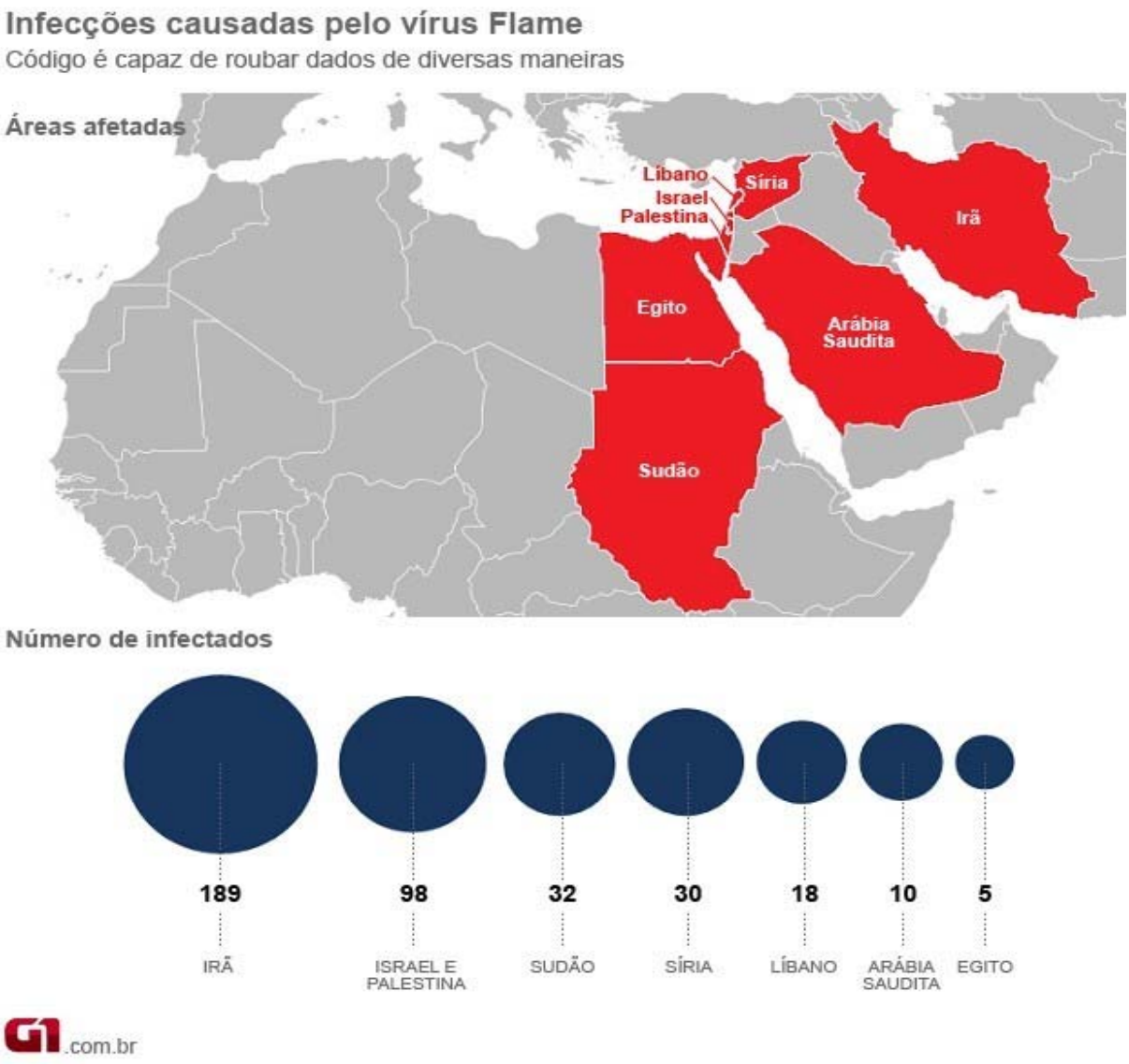


Figura 2 – Disseminação da ameaça Flame.
Fonte: ROHR, 2012.

O Stuxnet foi o *vírus* responsável por sabotar o programa de enriquecimento de urânio do Irã em Natanz, conforme noticiado no jornal *The New York Times.* Enquanto o *vírus* Flame, por sua vez, não possui nenhum componente para danificar sistemas, mas apenas para capturar dados. Segundo a Kaspesky, o Flame é muito mais complexo que o Stuxnet, pois ele possui um conjunto de módulos que pode ocupar mais de 40 vezes o espaço em disco que o Stuxnet utilizava (CARVALHO, 2012).

3 MÉTODOS, TÉCNICAS E FERRAMENTAS DE ATAQUES

Neste capitulo será abordado alguns métodos e técnicas mais importantes e algumas ferramentas utilizadas para realizar estes ataques.

3.1 MÉTODOS E TÉCNICAS USADOS EM UM ATAQUE CIBERNÉTICO

Com a proliferação das redes de computador no mundo aliado ao avanço tecnológico, os ataques cibernéticos têm se tornado mais complexos e perigosos. Diante disso, é necessário fazermos um estudo mais detalhado sobre alguns métodos e técnicas de ataque que podem ser usados para atingir uma organização ou uma nação.

3.1.1 Port Scanning

O *Port Scanning* é uma técnica de coleta de informações ou inteligência utilizada na fase de levantamento de informações, a qual é a primeira fase de um ataque e não caracteriza um ataque real.

Esta técnica é utilizada tanto por *hackers* quanto por administradores de redes, a fim de criar um mapa de todos os hosts ativos e com características interessantes para possíveis verificações, documentações ou escaneamentos mais precisos. Um dos softwares mais conhecido que faz *port scanning* é o nmap (BRADLEY, 2012).

Após a descoberta dos *Hosts* e identificação dos mais interessantes, o atacante passa para a fase de enumeração de serviços, podendo realizar um escaneamento de portas, para determinar seus serviços, versão e status. A partir das vulnerabilidades encontradas, é possível encontrar falhas de segurança, aumentando a chance de sucesso da invasão.

3.1.2 Engenharia Social

Com o crescimento do uso da internet e da tecnologia, as empresas estão investindo pesado na modernização de seus parques tecnológicos e na segurança deles, dificultando a exploração de vulnerabilidades e, com isso os invasores estão se especializando em explorar o fator humano, o qual é o principal problema da SI.

Nada adianta trancar as portas de sua casa, manter cadeados ou sistemas de segurança que monitorem ou dificultem a entrada pelas portas, sendo que alguém de dentro de casa sempre abre as portas para o bandido. Dessa maneira, todo investimento vai por água abaixo (ALVES, 2010).

A engenharia social é um método de ataque que utiliza o poder de influenciar e persuadir para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia (MITNICK; SIMON, 2003).

Não existe uma empresa totalmente segura, uma vez que a falta de conscientização dos funcionários e a total confiança em si e nos equipamentos de proteção da rede são os principais motivos deste tipo de ataque ser tão eficiente.

Para minimizar a possibilidade de ser uma vítima de engenharia social é necessário principalmente que haja divulgação constante da política de segurança da empresa, presença dos funcionários em cursos de capacitação e palestras de conscientização, regras severas de segurança das informações digitais e software de auditoria de acesso e monitoramento e filtragem de conteúdo (PEIXOTO, 2006).

Algumas técnicas mais utilizadas neste tipo de ataque:

3.1.2.1 Phishing

É a técnica de engenharia social mais utilizada que explora não uma falha do sistema e sim no fator humano, para se conseguir acesso à rede-alvo ou informações sigilosas, por meio de *e-mails* manipulados e enviados às organizações e pessoas, com o intuito de aguçar algum sentimento que faça com que o usuário leia o *e-mail* e realize as operações solicitadas (RAFAEL, 2013).

A maioria dos p*hishings* possui algum anexo ou *links* dentro do *e-mail* que direcionam para a situação que o atacante deseja, e com as informações levantadas, é possível continuar o ataque mais direcionado.

3.1.2.2 Dumper Driver ou Trashing

É a técnica utilizada para conseguir informações privilegiadas que potencializem as tentativas de quebra de senha e invasões, por meio da procura de informações em lixeiras, aproveitando a falta instrução dos usuários e técnicos no descarte de informações sigilosas.

Para diminuirmos o risco de acesso não autorizado, perda ou roubo de informações, devemos seguir regras de descarte da informação de acordo com o seu grau de sigilo, utilizar os trituradores de papel, apagar as trilhas magnéticas do Disco Rígido (HD) [22], fazer a manutenção do lixo nas áreas de acesso restrito, acompanhar todos os visitantes enquanto estiverem no local e realizar a política de mesa limpa de papeis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação[23].

---

[22] Disco Rígido (*Hard Disk*) - É um sistema de armazenamento de alta capacidade, que permite armazenar arquivos e programas (MUSEU, 2004).

[23] Política da Mesa limpa e tela Limpa definem diretrizes que reduzem o risco de uma violação de segurança, perda e roubo de informações, causados por documentos digitais ou escritos à mão

3.1.3 Denial-of-Service *(*DoS*)*

Os ataques de negação de serviço são feitos não com o objetivo de invadir o sistema, mas sim com o propósito de torná-lo indisponível, por meio do consumo total da largura de banda de uma rede específica ou por inanição de recursos, onde o ataque se dá pelo consumo de todos os recursos do sistema, fazendo com que ele deixe de responder a requisições de usuários válidos.

Apesar de não causarem a perda ou roubo dos dados, os ataques DoS são graves, pois deixa a rede indisponível quando um usuário precisa utilizá-la, ferindo uma das propriedades essenciais da SID, a qual garante que a informação estará disponível para o usuário e para o sistema de informação que está em operação no momento que a organização requer (ISO 27002, 2005).

A gravidade deste ataque está relacionada ao tempo do sistema estar fora do ar, à perda de credibilidade e ao trabalho físico envolvido em identificar e reagir a tais ataques.

Este método de ataque pode ser realizado em redes cabeadas e em redes sem fio. Nestas últimas, como todos os equipamentos sem fio utilizam a mesma frequência, então quando funcionam próximos podem causar degradação do sinal, fazendo com que a capacidade e a qualidade diminuam. Diante disso, o atacante, com o equipamento apropriado, pode enviar uma grande quantidade de trafego aleatório na mesma frequência do roteador, fazendo fazer com que a rede fique indisponível.

---

deixados sobre a mesa ou em impressoras, acesso a computadores sem senha de proteção de tela, ou mesmo, acesso a dispositivos removíveis expostos em locais desprotegidos (ISO 27002, 2005).

No entanto, existem ataques mais sofisticados, como por exemplo, um atacante se passando por um ponto de acesso com o mesmo ESSID[24] (*Extended Service Set Identifier*) e endereço MAC[25] de outro ponto de acesso válido enchendo a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se reassociarem. Enviando as requisições de dissociação em períodos curtos de tempo, o DoS é concretizado, uma vez que os clientes não conseguiriam permanecer conectados por muito tempo (DUARTE, 2003).

Algumas técnicas de DoS:

3.1.3.1 Distributed Denial-of-Service (DoS)

Este ataque é a soma de dois conceitos do mundo da TI: negação de serviço e computação distribuída (SACHDEVA; SINGH; SINGH, 2011).

Embora os ataques de DDoS já existam há mais de uma década, a dimensão e a frequência desses ataques estão aumentando mais rápido do que a capacidade da maioria das organizações de absorvê-los.

O ataque DDoS é dado, basicamente, em três fases: uma fase de levantamento das vulnerabilidades das redes-alvos e exploração, que é o objetivo de obter acesso privilegiado nessas máquinas.

Na segunda fase, o atacante instala *software* DDoS nas máquinas invadidas (agentes), com o intuito de montar a rede de ataque. E, por último, a fase onde é lançado algum tipo de inundação de pacotes contra uma ou mais vítimas, consolidando efetivamente o ataque.

---

[24] ESSID (*Extended Service Set Identifier*) – É o nome da rede, que deve ser conhecido tanto pelo concentrador quanto pelo cliente que deseja conexão (RUFINO, 2011)

[25] Endereço MAC - É o endereço físico da placa de rede, conforme disponível em http://www. mundodoshackers.com.br/o-que-e-um-endereco-mac (TÁCIO, 2010).

Assim que o atacante ordena o ataque, uma ou mais máquinas vítimas são bombardeadas por um enorme volume de pacotes, resultando não apenas na saturação do *link* de rede, mas principalmente na paralisação dos seus serviços.

A figura 3 e dada uma clara visão de como é feito um ataque DDoS.

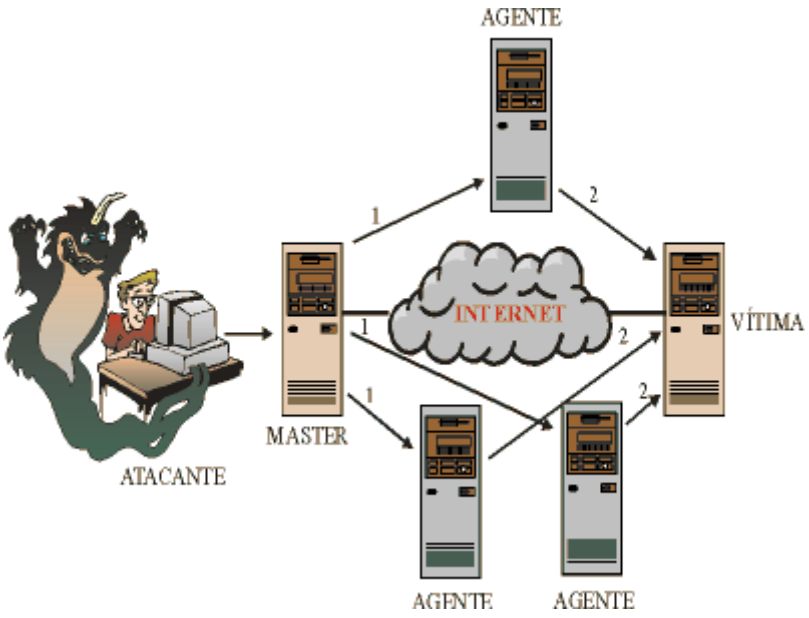


Figura 3 – Ataque DDoS .
Fonte: SOLHA, 2004.

Em um mundo em constante crescimento, cada vez mais interconectado e complexo, pode ser difícil para as organizações se anteciparem ao próximo ataque ou atividade maliciosa, então existem alguns passos que podem ser tomados para tornar efetiva a detecção. Algumas anomalias podem sinalizar a ocorrência deste tipo de ataque. São elas:

1. Excesso de tráfego: Aumento repentino de atividades de processamento e consumo total da banda, ultrapassando o número de acessos esperado.

2. Pacotes UDP[26] e ICMP[27] de tamanho anormal: Grande parte das sessões UDP utilizam pacotes mínimos de dados com tamanhos entre 512 e 1280 bytes. As mensagens ICMP são de tamanhos diferenciados não sendo maiores de 128 bytes. Pacotes de dados que saiam desses padrões podem ser considerados suspeitos de terem códigos maliciosos e estarem participando de um ataque (principalmente se forem em grandes quantidades).

3. Pacotes TCP e UDP que não fazem parte de uma conexão: Alguns ataques do tipo DDoS fazem uso vários protocolos aleatórios para enviar dados sobre meios não orientados à conexão. A detecção pode ser realizada empregando um *statefull firewall*[28].

4. Pacotes binários: Quando os dados de pacotes forem recebidos somente em dados binários e o seu destino for para diferentes protocolos, eles devem ser analisados e, dependendo do caso, descartados. Pacotes binários podem estar escondendo algum comando de controle de máquina embutido em seu código binário.

Segundo Maia (2003), ainda hoje não existe uma solução definitiva para este tipo de ataque. O que existem são métodos que podem ser concatenados e utilizados para minimizar os riscos e proteger um determinado sistema. Para isso é necessário:

• Aumentar o nível de segurança dos ativos de rede, realizando as atualizações de segurança, instalando *patches* que possam fechar as brechas de vulnerabilidades conhecidas, a fim de dificultar a formação das redes DDoS;

---

[26] *User Datagram Protocol* (UDP) - É um protocolo orientado à transação, que provê um serviço sem conexão, não garantindo a entrega e duplicação dos pacotes. (RFC 768, 1980).

[27] I*nternet Control Message Protocol* (ICMP) - É um protocolo usado para relatar um erro no processamento de datagramas, utilzando o suporte de base do IP. (RFC 792, 1981).

[28] *Statefull-firewall* - É um Firewall que mantém o estado das conexões (NORTHCUTT, 2005).

• Implementar mecanismos *anti-spoofing* para evitar a movimentação de pacotes com endereços falsificados pela internet; e

• Limitar a banda disponível para os pacotes utilizados no ataque, por meio de configurações nos equipamentos de conectividade.

3.1.3.2 Distributed Reflection Denial-of-Service (DDoS)

Este novo tipo de negação de serviço que se aproveita de duas falhas em serviços de internet, a falsificação da origem (IP *Spoofing*) e servidores DNS recursivos abertos, pois menos *botnets* são necessários para gerar grandes volumes de tráfego de ataque, devido às técnicas de reflexão e ampliação (DUNN, 2013).

Impulsionados pela facilidade de obter listas de servidores vulneráveis para ser usado em ataques aliado ao alto grau de anonimato, fazem com que os cibercriminosos mudem suas táticas em ataques DDoS e consigam ser bem mais devastadores. Tal fato levou os principais veículos de imprensa internacional, como a BBC e o *New York Times*, a noticiarem como o maior ataque cibernético da história, que deixaram a internet inteira lenta (LINHA DEFENSIVA, 2013).

De acordo com pesquisa feita pela Empresa de mitigação Prolexic, baseada no levantamento do terceiro trimestre de 2013, estes ataques de reflexão tiveram um aumento de 265% comparado com o mesmo período de 2012, afirmou o presidente da Prolexic, Stuart Scholly (SEGINFO, 2013).

Para realizar este ataque, as máquinas escravas enviam um fluxo de pacotes, com o endereço de origem falsificado, para outras máquinas não infectadas, conhecidas como refletores, os quais conectam com a vítima e enviam um grande volume de tráfego. O ataque é montado pelas máquinas não comprometidas (refletores) sem estarem cientes da ação.

O sequestro de intermediários para amplificar o efeito fez com que este projeto criasse duas vítimas, o alvo pretendido e o intermediário (HENRIQUE, 2013), conforme mostrado na figura 4 abaixo.

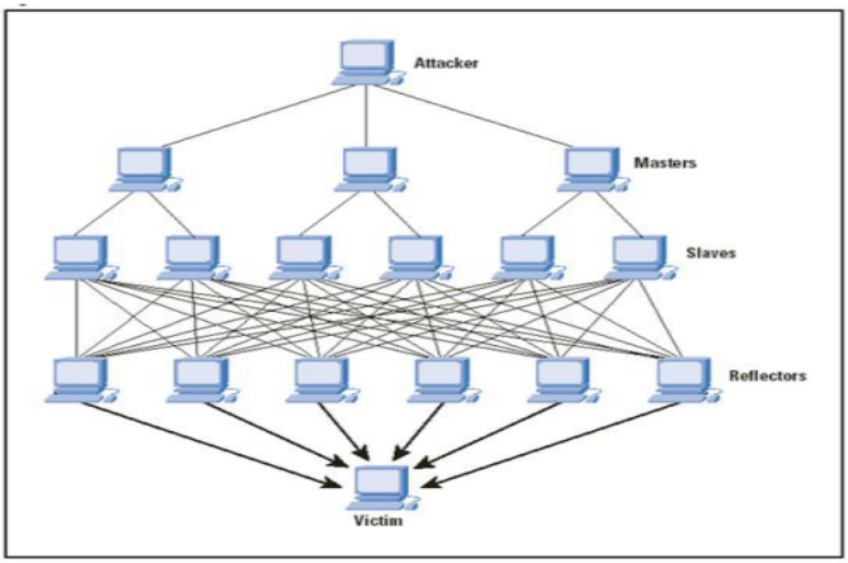


Figura 4 – DRDoS.
Fonte: FERRAZO, 2011.

3.1.3.3 SYN Flood ou TCP SYN Flood

É uma técnica de ataque DoS, que atua na requisição de abertura de conexões TCP[29], onde o atacante envia para o servidor-alvo uma grande quantidade de pacotes SYN[30] (SCHLEMER, 2007).

Quando é feita qualquer requisição TCP a um servidor, há uma troca de pacotes e comumente conhecida como o processo de *handshake* de três vias (*Three-Way Handshake*) [31], conforme mostrado na figura a seguir.

[29] *Transmission Control Protocol* (TCP) - É um protocolo orientado à conexão e fornece um serviço de entrega de pacotes confiável (RFC 793, 1981).
[30] Pacotes SYN - É uma solicitação de sincronização enviada pelo cliente ao servidor para estabelecer o sincronismo (SCHLEMER, 2007).
[31] *Three-Way Handshake* - É o processo para estabilizar a conexão TCP/IP entre o cliente e o servidor (TCP/IP GUIDE, 2005).

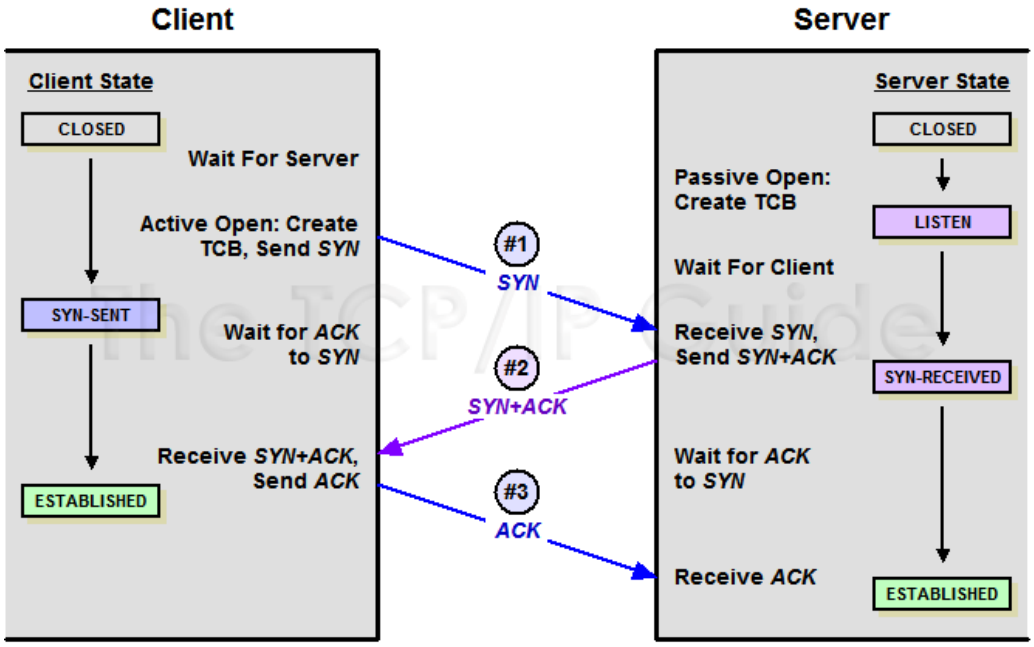


Figura 5 - Three-Way Handshake.
Fonte: TCP/IP GUIDE, 2005.

Este processo é iniciado quando cliente envia uma solicitação de sincronização com o *flag* SYN ativado, no campo *flag* do header TCP, com número de sequência 0 (Seq=0), para o servidor.

Se o servidor quiser e puder atender, ele devolve ao cliente uma solicitação de sincronização com os *flags* de SYN e de ACK ligados e com número de sequência 0 (Seq=0). Esta segunda etapa é conhecida como SYN/ACK.

Se o cliente ainda quiser manter a conexão, devolve ao servidor um terceiro pacote sem dados, apenas com o *flag* de ACK ligado (SYN desligado) e o número de sequência 1 (Seq=1).

Somente após esta etapa é que os dados podem ser trocados (SCHLEMER, 2007).

O mais importante para entender a gravidade do ataque é saber que o servidor, ao receber o primeiro pacote (SYN), se ele quiser, precisa antes de

responder com o SYN/ACK, alocar recursos de hardware para atender esta nova conexão.

Como o TCP é um protocolo confiável, que trata de desordenamento e perdas de pacotes, estes recursos não são poucos, pois envolvem buffers de envio e de recebimento, controle de números de sequência, relógios, enfim, muitos recursos de memória, principalmente.

Nesta técnica de ataque, o atacante gera quantos SYN a máquina dele for capaz e não responde nenhum deles, então o servidor alocará recursos para cada um, como se fossem requisições legítimas, só desalocando quando acabar o tempo.

Atualmente, temos hardware com capacidades de memória e recursos gigantescos, mas não existem recursos infinitos. Mais cedo ou mais tarde os recursos se esgotarão e o servidor ficará incapaz de atender clientes legítimos.

Um ataque de *SYN Flood* e feito utilizando IP de origem falsificado (*spoofing*), para que o atacante não receba os ACKs de suas falsas solicitações (CARNEGIE, 2000).

Existem medidas que podem prevenir estes ataques em alguns servidores. A solução por *firewall* não é o suficiente para resolvermos este tipo de ataque, então a técnica de *SYN Cookies*[32] permite que o servidor escolha o seu número de sequência por meio de uma função *hash* de 32 bits, onde serão consideradas informações como IP/Porta do cliente e dados que só o servidor tem. O servidor gera este número e não aloca recursos (RFC 4987, 2007).

[32] SYN *Cookies* – É a técnica de proteção usada contra os ataques de SYN *Flood*. Número de sequencia de 32 bits codificado com uma função *hash* inserido no SYN-ACK pelo servidor (RFC 4987, 2007).

Quando vier o último pacote do *Three-Way Handshake*, o servidor refaz o cálculo do *Hash*, e verá que nenhum dado foi alterado, podendo concluir que o cliente é legítimo.

Com esta técnica, o atacante está impossibilitado de realizar o ataque de *SYN Flood*, pois ele não recebe o pacote SYN/ACK, pois como ele falsificou o IP (*spoofing*), então este pacote foi para o IP falso. Logo o atacante não conhece o valor do número de sequência do servidor para poder devolvê-lo incrementando de um, como realizado no segundo passo do *Three-Way Handshake* (RFC 4987, 2007).

Só resta ao atacante tentar quebrar o *hash* de 32 bits, o que não é uma tarefa difícil, mas precisaria de uns 3 segundos para quebrar, isto já é uma eternidade para que o *SYN Flood* realmente cause uma negação de serviço.

No Linux, isso pode ser evitado, ativando o uso do recurso oferecido diretamente pelo *Kernel*[33], por meio da inclusão do seu script no firewall e ativação do TCP *syncookie* no *kernel*.

Ao ativar o recurso, o sistema passa a responder ao pacote SYN inicial com um *cookie*, que identifica o cliente. Com isso, o sistema aloca espaço para a conexão apenas após receber o pacote ACK de resposta, tornando o ataque sem sucesso. O atacante ainda pode consumir um pouco de banda, obrigando o servidor a enviar um grande volume de SYN *Cookies* de resposta, mas o efeito sobre o servidor será mínimo (MORIMOTO, 2010).

3.1.3.4 UDP Flood

É uma técnica de ataque DoS, diferenciada do TCP SYN *Flood*, porque a comunicação UDP não estabelece conexão, ou seja, não faz o *Three-Way*

[33] *Kernel* - É uma série de arquivos escritos em linguagem C e em linguagem *Assembly* que constituem o núcleo, o centro de todas as atividades desempenhadas pelo sistema operacional (PIRES, 2007).

Handshake. Por esse motivo, o atacante pode enviar pacotes UDP aleatórios para todas as portas que porventura estejam abertas no servidor (SOLHA, 2004).

Quando o servidor recebe os pacotes UDP enviados pelo atacante, ele tenta tratar e determinar as requisições feitas naquelas determinadas portas em que foram recebidos os pacotes. Porem, quando o servidor verifica que não existe nenhuma aplicação aguardando tal pacote recebido, ele então emite um pacote ICMP para o destinatário (provavelmente para um endereço IP falso ou forjado), comunicando o fato de não ter encontrado o pacote no serviço solicitado. Quando esses pacotes são em grande quantidade, o sistema poderá ser comprometido causando assim uma negação de serviço.

3.1.3.5 Smurf

O *Smurf* é uma técnica de ataque de DoS, com o objetivo não de parar só um computador, mas sim uma rede inteira (BOFF, 2009).

O atacante envia tráfego ICMP *echo request (ping)*[34] para um IP de broadcast[35] da rede, utilizando o endereço de origem falsificado da vítima. O roteador receberá os ICMP *echo request* e redirecionará para todos os hosts da rede.

Esta técnica faz com que cada computador da rede responda aos falsos pacotes de *ping* e envie uma resposta (ICMP *echo reply*) ao computador de destino, inundando-o (SYMANTEC, 2014), resultando em degradação do serviço, ou mesmo, negação de serviços para aquele segmento de rede, dado o elevado volume de tráfego gerado.

---

[34] *Ping* – É uma sigla para *Packet InterNet Grouper*. É um comando capaz de medir quantos milissegundos (ms) um pacote de informações leva para ir até um destino e voltar (GUILHERME, 2012).

[35] Endereço de *broadcast* - É o endereço comum usado para transmitir uma mensagem a todos os hosts em uma rede (SYMANTEC, 2014)

Em muitos casos, os administradores de rede podem evitar que suas redes sejam utilizadas como amplificadores[36], bloqueando nos *firewalls* a entrada de pacotes ICMP/UDP que tenham como destino o endereço de *broadcast* da rede e desativar os serviços que não estão sendo utilizados pelos computadores de rede (BOFF, 2009).

3.1.3.6 Fraggle

Esta técnica de ataque semelhante ao *Smurf*, a qual utiliza pacotes UDP. Em vez de enviar pacotes de ICMP *echo response*, ele envia pacotes UDP, com endereço de origem falsificado, para os endereços de *broadcast* da rede. As máquinas da rede ao receberem o pacote UDP respondem à vítima, a qual envia mais uma resposta, gerando uma grande quantidade de tráfego na rede (BOFF, 2009).

3.1.3.7 Ping Flood

Este método de ataque é um dos mais antigos e simples, mas não muito eficaz atualmente, uma vez que o seu objetivo é saturar a rede com tráfego ICMP *Echo Request*, exigindo que a vítima gaste todo seu tempo de CPU para responder os pacotes falsos. (TOMICKI, 2010).

Este ataque envia um pacote mal formado explorando uma falha do sistema, sendo reforçado por meio do envio de pacotes grandes (superior a 65536 octetos), forçando os roteadores de borda a gastar muito tempo para realizarem a fragmentação destes pacotes.

---

[36] A rede está sendo usada como amplificador quando não só aceita ICMP *echo requests* enviados para um endereço de broadcast, mas que permite ICMP *echo replies* enviados para fora (BOFF, 2009).

Algumas maneiras de se proteger é filtrando a entrada de pacotes ICMP *Echo Request* na rede, bloquear pacotes acima do tamanho limite no *firewall* ou no IDS (TOMICKI, 2010) e aplicar o último *patch* de atualização do Sistema Operacional.

3.1.4 Man-in-the-Middle (MITM)

Este método de ataque consiste basicamente em o atacante se infiltrar na comunicação entre duas partes, interceptar os dados, manipulá-los e retransmiti-los sem que nenhuma das partes perceba (JORGE, 2011).

Segundo Kaspersky (2013), uma variante deste método de ataque e a forma mais comum de MITM, o atacante, com o objetivo de roubar informações, usa um roteador sem fio como mecanismo para interceptar o tráfego de dados existente na comunicação de suas vítimas, o que pode acontecer tanto por meio de um roteador corrompido quanto por falhas na instalação do equipamento.

Numa situação comum, o atacante configura o seu dispositivo wireless para atuar como *access point* (AP) e o nome com um título comum em redes públicas. Então quando um usuário se conecta ao roteador e tenta navegar em sites com informações sigilosas, como banco ou comércio eletrônico, o invasor rouba suas credenciais.

Num caso recente noticiado no blog da empresa Kaspersky, um hacker usou vulnerabilidades na implementação de um sistema criptográfico de uma rede WiFi real e a usou para capturar informações. Esta é a situação é mais incomum, mas também a mais lucrativa, pois se o atacante for persistente e acessar o equipamento hackeado por algum tempo, ele terá a possibilidade de capturar as sessões de seus usuários e, com isso, ter acesso às suas informações sigilosas.

Existem diferentes maneiras de defender-se dos ataques MITM, mas a maioria delas deve ser instalada nos roteadores e servidores e não são totalmente seguras.

Uma delas é aplicar uma criptografia complexa entre o cliente e o servidor, sendo que o servidor pode identificar-se apresentando um certificado digital para que o cliente possa estabelecer uma conexão criptografada e, assim, enviar a informação sensível. Mas esta possibilidade de defesa depende de que ambos servidores tenham tal criptografia habilitada.

Da mesma forma, os usuários também podem se prevenir de ataques MITM da seguinte forma:

- evitar se conectar a WiFi livres;
- instalar *plugins*, como HTTPS Everywhere ou ForceTLS em seu navegador, uma vez que estes programas selecionarão apenas conexões seguras sempre que estas estejam disponíveis (KASPERSKY, 2013);
- utilizar, sempre que possível, SSL/TLS[37] em suas conexões, principalmente em conexões irão ser transmitidos dados importantes;
- verificar certificados SSL antes de usá-los; e
- utilizar dispositivos de autenticação, como *tokens* ou outras formas de autenticação de dois fatores, para acessar contas que contenham informações sensíveis e confidenciais.

3.1.5 Web Defacement

Este método de ataque, também conhecido como pichação de site, é teoricamente simples e pode colaborar para uma ação mais complexa a ser

[37] SSL/TLS – São protocolos que permitem a comunicação segura na internet. O TLS é o sucesor do SSL (SAUVAGE, 2014).

executada no alvo. Geralmente estes ataques tem uma intenção política ou de inteligência, a fim de desestabilizar o adversário, afetando seu emocional, alertar para um sistema não crítico da ação a ser executada, desviando a atenção do real alvo.

Neste ataque o hacker explora vulnerabilidades e *bugs* de segurança em páginas da *web* para modificá-las, como por exemplo, algum código HTML errado, algum formulário de contato mal configurado, página índex com erros na codificação. Diante desta brecha, o atacante insere um código malicioso que faz a troca da página principal do site, outras vezes, ele identifica o IP do servidor onde está hospedado o site e insere o código malicioso (REYES, 2010).

A solução para evitar novos ataques deste tipo é inserir alguns códigos de segurança na página, fechar toda brecha de codificação e desabilitar os serviços desnecessários que estão rodando no servidor *web*.

Em 2011, uma onda de invasões de *hackers* em sites oficiais nos Estados Unidos e Europa atingiram os sites brasileiros. As páginas do Governo Federal, da Presidência da Republica e de algumas empresas foram alvos de ataques da versão brasileira do grupo *hacker* LulzSec. Os ataques congestionaram as redes onde as páginas estavam hospedadas, deixando os sites fora do ar durante um curto período. O objetivo do grupo era roubar informações sigilosas e expô-las na internet (VERLY, 2011).

3.2 FERRAMENTAS DE ATAQUE

Atualmente, constatamos que os ataques cibernéticos vêm se tornando um problema cada vez mais grave no mundo, pois novas técnicas e ferramentas surgem

a cada instante e estão mais eficientes. Diante disso, vamos analisar mais detalhadamente alguns artefatos de ataque.

3.2.1 Varredura de rede

É um dos primeiros para passos do atacante para fazer o levantamento das vulnerabilidades da vítima, mas também pode ser usado por administradores de rede, a fim de tornar seus ativos de rede mais seguros. As ferramentas mais usadas são detalhadas abaixo:

3.2.1.1 Nmap e Nessus

São as melhores ferramentas livres utilizadas para fazer uma varredura na rede e auditoria de segurança, que permitem verificar algumas características da rede, status de serviços que estão rodando nos hosts, informações sobre o seu Sistema operacional.

O Nessus possui versão paga e *free*, funcionando por meio de *pluggins* instalados e indica as vulnerabilidades detectadas e os passos que devem ser seguidos para eliminá-las.

3.2.1.2 Aircrack-ng e Aerodump

É uma suíte de ferramentas relacionadas à *wardriving* utilizadas para captura de redes sem fio 802.11[38], onde é possível mapear, traçar e quebrar a chave destas redes.

O aerodump-ng é usado para capturar pacotes de dados brutos em redes sem fio, coletando informações dos *Access Points* (AP) e computadores detectados

[38] O padrão IEEE 802.11 foi projetado para oferecer comunicação sem fio com alta largura de banda, fornecendo serviços que podem migrar de uma célula para outra com frequência, ou seja, é um padrão criado para lidar com mobilidade (TANENBAUM, 2003).

e gravando em um arquivo, para posteriormente injetar os *frames*, utilizando o Aireplay-ng e, em seguida, fazer o ataque para quebra da senha com o Aircrack-ng.

3.2.1.3 Nikto

É um software de código aberto, instalado no Backtrack 5[39], usado como scanner de vulnerabilidades em servidores *Web*, sendo possível verificar as configurações destes servidores, como os arquivos *índex* e opções do servidor HTTP.

3.2.2 Negação de serviço

É um ataque em que o inimigo consegue colocar um sistema-alvo inutilizável ou sobrecarrega-o, de modo que não pode ser utilizado por usuários legítimos. Existem várias ferramentas que podem ser utilizadas para este tipo de ataque e algumas serão detalhadas abaixo:

3.2.2.1 Trinoo

O Trinoo (ou Trin00) é uma ferramenta de ataque, usada para lançar ataques do tipo DDoS, especialmente para ataques do tipo UDP *flooding*.

Originalmente ela foi desenvolvida para Sistemas Operacionais Solaris 2.X ou Linux, porém, com a sua evolução, foram aparecendo também para plataformas Microsoft Windows (MARTINEZ, 2000).

Segundo Dittich (2009), o esta ferramenta é dividida em duas partes, a parte controladora (*master*) e a parte que é controlada (*client*). O componente *master*

[39] BackTrack 5 - é um Sistema Operacional Linux que possui mais de 300 ferramentas diferentes e atualizadas, que são logicamente estruturadas de acordo com o fluxo de trabalho de profissionais de segurança, utilizado para realizar testes de segurança e de penetração, conforme disponível em http:// www.backtrack-linux.org.

possui uma unidade controladora do Trinoo que é secretamente instalada no computador da vítima. Essa unidade tem a missão de distribuir muitos pacotes UDP destinados a um determinado servidor.

Ao tentar processar tais pedidos, respondendo com uma mensagem "ICMP *Port Unreachable*" para cada pacote UDP invalido recebido, este servidor esgota seus recursos, o que resulta numa recusa de serviço (DoS).

O Trinoo também possui um componente cliente que é usado para controlar um ou mais componente *master* remotamente e enviar vários comandos.

A comunicação entre o *master* Trin00 e os agentes é feita via pacotes UDP na porta 27444/udp ou via pacotes TCP na porta 1524/tcp. A comunicação entre os agentes e o *master* Trin00 também é através de pacotes UDP, mas na porta 31335/udp. Quando um *daemon* é inicializado, ele anuncia a sua disponibilidade, enviando uma mensagem ("*HELLO*") ao *master*, o qual mantém uma lista dos IP das máquinas agentes ativas, que ele está controlando (DITTRICH, 2009).

3.2.2.2 Tribe Flood Network (TFN)

O TFN é uma ferramenta usada para lançar ataques DoS coordenados em direção a uma ou mais vítimas, a partir de várias máquinas comprometidas, da mesma forma que o Trinoo. Além de serem capazes de gerar ataques do tipo UDP flood, uma rede TFN pode gerar ataques do tipo SYN *flood*, ICMP *flood* e *Smurf/Fraggle*. O atacante não precisa se conectar ao operador (MCCLURE, 2003).

Neste tipo de ataque é possível forjar o endereço do remetente dos pacotes lançados às vítimas, o que dificulta qualquer processo de identificação do atacante.

No caso especifico de lançar o ataque *Smurf/Fraggle* para atingir a(s) vítima(s), a inundação de pacotes é enviada às redes intermediarias, as quais consolidarão o ataque.

O controle remoto do componente master TFN é realizado por meio de comandos executados pelo programa cliente. A conexão entre o atacante e o cliente pode ser realizada usando qualquer um dos métodos de conexão conhecidos, tais como: RSH, RLOGIN e TELNET[40].

A comunicação entre o cliente TFN e os *daemons* é feita via pacotes ICMP *echoreplay*, não existindo comunicação TCP ou UDP entre eles.

Não é necessário inserir senha para executar o cliente, no entanto, e indispensável à lista dos IP das máquinas que tem os *daemons* instalados. Algumas versões da aplicação cliente usam criptografia para ocultar o conteúdo desta lista (DITTRICH, 1999).

3.2.2.3 Stacheldraht

É uma ferramenta de ataque usada para lançar ataques DDoS que combina características do Trinoo e do TFN, adicionando a criptografia simétrica da comunicação entre o atacante e o *master* e atualização automática dos agentes (SOLHA; TEIXEIRA; PICCOLINI, 2000).

Como seu predecessor TFN, ela também é capaz de gerar ataques DoS do tipo UDP *flood*, TCP *flood*, ICMP *flood* e *Smurf/fraggle*.

A ideia de criptografia da comunicação entre a unidade controladora e a unidade controlada surgiu devido à deficiência encontrada nas ferramentas

[40] RSH, RLOGIN e TELNET - permitem acessar remotamente outro computador, mas as conexões não utilizam criptografia, então os dados trafegam de forma desprotegida e caso exista algum *sniffer* na rede, poderá capturar todo o tráfego.

anteriores, onde a conexão entre eles era completamente desprotegida, estando exposta ao ataque de roubo de sessão (TCP *Session Highjacking*[41]) (SOLHA; TEIXEIRA; PICCOLINI, 2000).

A comunicação entre o *cliente* e o *master* é feita via pacotes TCP na porta 16660/tcp e entre o master e o cliente via pacotes ICMP *echoreplay* na porta 65000/tcp.

3.2.2.4 T50

É uma ferramenta simples e poderosa de injeção de pacotes, desenvolvida pelo brasileiro Nelson Brito, capaz de fazer ataques DoS e DDoS, usando o conceito de *stress testing*. Com ele você pode enviar um número altíssimo de requisições de pacotes, de tal forma que o alvo não consiga atender todas as requisições ou as atenda de forma lenta, dessa forma o alvo pode cair ou ficar lento em poucos segundos (TÁCIO, 2011).

Ela funciona utilizando um único *socket*, com suporte a múltiplos protocolos e foi acoplada ao BackTrack 5 como uma ferramenta para teste de saturação em redes.

Atualmente o T50 é capaz de emitir mais de 1 milhão de pacotes por segundo de SYN *Flood*, congestionando 50% do *uplink* de uma rede 1000BASE-T (*Gigabit Ethernet*). E ainda pode enviar requisições de pacotes dos protocolos ICMP, IGMP, TCP e UDP sequencialmente com diferença de microssegundos (TÁCIO, 2011).

---

[41] Roubo de sessão (TCP *Session Highjacking*) - é ato de controlar uma sessão de comunicação TCP/IP válida entre computadores, explorando uma falha do protocolo TCP e, pelo fato preponderante de que, na maior parte das vezes, a autenticação somente ocorre no início de cada sessão.

3.2.2.5 Slow Loris

Uma técnica de ataque de negação de serviço, na qual o script é feito para abrir de maneira simples uma sessão HTTP (*HyperText Transfer Protocol)* e mantê-la aberta por muito mais tempo do que normalmente ficaria.

O script funciona como se pessoas estivessem na fila para o pagamento de suas compras em uma loja, onde cada um encontra com seu caixa (*sockets*) e pagam suas compras em centavos, tomando muito tempo.

Esta ferramenta utiliza os cabeçalhos HTTP e mantém adicionando um novo cabeçalho a cada 5, 10 ou 299 segundos. Então o Apache não tem memória suficiente, pois quando cada novo cabeçalho é adicionado, o contador do *timeout* é reiniciado (IMAISUMI; MARTINS, 2013).

Com essa técnica é possível bloquear cada tarefa do servidor levando o servidor *web* a uma completa parada. Isso porque por padrão a configuração do *timeout* do Apache é de 300 segundos, assim, cada cabeçalho adicionado pode alargar o tempo de saída (RSNAKE 2013).

Em relação à auditoria, este artefato de ataque não mostrará que o servidor está sofrendo um ataque, da mesma forma que as mensagens de *log* de erros no servidor serão escassas.

A CPU estará parada, sem operações de entrada e saída no disco e dificilmente será possível visualizar qualquer tráfego na rede. O que será possível observar será um enorme número de conexões de redes abertas como *status* de estabelecida.

3.2.3 Interceptação de conexão

Este tipo de ataque é o mais clássico, em que o atacante se insere no meio da comunicação entre duas entidades, sem que estas tenham conhecimento que a ligação entre ambas está comprometida. Neste tópico estudaremos algumas ferramentas utilizadas para este tipo de ataque:

3.2.3.1 Ethercap

É uma ferramenta classificada como *sniffer*[42], que pode ser usada para ataque de MITM em redes local e também para fazer auditoria de segurança.

Ele é capaz de interceptar o tráfego de um segmento de rede, capturando senhas e conduzindo escutas contra certo número de protocolos comuns.

Esta ferramenta pode ser usada para realizar ataques ARP *Poisoning*[43], colocando a interface de rede em modo promíscuo e fazendo envenenamento ARP nas máquinas alvo. Da mesma forma, pode executar os ataques de DNS *spoofing*[44], além de poder ser usada em conjunto com o SSLStrip, a fim de capturar o trafego HTTPS/SSL[45].

3.2.3.2 SSLStrip

Ao longo dos anos, percebemos que o uso de uma conexão segura HTTPS não garante a proteção total do usuário, uma vez que existem métodos que possibilitam o roubo de informações mesmo em sites seguros, quer por meio da

---

[42] *Sniffer* - É uma ferramenta capaz de capturar todo o tráfego de uma rede (GALOSSI, 2012).
[43] ARP *Poisoning* (ou *ARP-Spoofing*) - É o meio mais eficiente de executar o ataque MITM, o qual permite que o atacante intercepte informações confidenciais posicionando-se no meio de uma conexão entre duas ou mais máquinas. Só é aplicado em redes Ethernet (com fio) (VIEIRA, 2009).
[44] DNS *Spoofing* - É a técnica de ataque em que o hacker pode determinar para qual site o usuário vai ser redirecionado quando acessar um determinado dominio (GALOSSI, 2012).
[45] HTTPS/SSL - São protocolos que permitem a comunicação segura na internet (SAUVAGE, 2014).

instalação de certificados falsos ou por enganar o alvo se fazendo passar por um Proxy (GALOSSI, 2013).

O SSLStrip é relativamente fácil de aplicar e extremamente poderoso, que permite a captura de tráfego HTTPS/SSL e funciona com a técnica de ARP *Spoofing*[46].

A lógica do SSLstrip é bem simples, ele altera todos os GET HTTPS de uma página por HTTP, e por meio de um ataque MITM, faz com que a Vítima e o Atacante se comuniquem via HTTP, quando na verdade o Atacante e o Servidor estão se comunicando via HTTPS (GALOSSI, 2013).

Para evitar ataques do tipo MITM existe um *daemon* chamado ArpON (ARP *Handler Inspection*), que funciona monitorando a tabela ARP da rede, gerando e bloqueando as alterações na tabela (GALOSSI, 2013).

Ele também é capaz de detectar e bloquear ataques mais alarmantes como DHCP *Spoofing*[47], DNS *Spoofing*, *WEB Spoofing*[48], *Session Hijacking*[49], SSL/TLS *Hijacking*[50] (PASQUALE, 2011).

Segundo Galossi (2013), é instalado no servidor que compartilha a Internet para a rede interna, e nele é colocado todos os IP e MAC dos clientes. Assim,

---

[46] ARP *Spoofing* - Consiste em adicionar ou substituir, na tabela ARP da maquina alvo, uma entrada IP da máquina alvo = MAC do atacante. Com isso quando a máquina alvo for montar o pacote para envio, ela montará com o IP real do servidor de destino, porém utilizará o endereço MAC do atacante, ou seja, quando este pacote passar pelo switch, será encaminhado para o atacante (GALOSSI, 2012).

[47] DHCP *Spoofing* - Ocorre quando um atacante responde a solicitações DHCP, listando-se como o gateway padrão ou servidor DNS. DHCP *Snooping* é o recurso de segurança que, quando ativado, permite que somente portas confiáveis de uplink para um servidor DHCP são autorizadas a passar o tráfego DHCP, as outras são bloqueadas (AARON, 2010)

[48] WEB *Spoofing* - Permite que um atacante crie uma cópia da página web e os acessos são canalizados através de computador do invasor, permitindo que o invasor para monitorar todas as atividades da vítima (FELTEN at. Al, 1997).

49 Session - Consiste na exploração do mecanismo de controle de sessão web, roubando ou prevendo um token de sessão válido para obter acesso não autorizado ao servidor *web* (OWASP, 2011).

50 SSL/TLS *Hijacking* – Consiste em, inicialmente, fazer um ataque MITM em uma derminada rede, permitindo ao atacante ter acesso a todo tráfego HTTPS e, com isso, descriptografar os cookies dos usuários e roubar as suas sessões (KUMAR, 2012).

quando o atacante tentar fazer o ARP *spoofing*, ele não conseguirá completar. Do alvo para o gateway[51], ele vai conseguir, pois não temos nenhuma proteção no cliente, mas quando ele tentar fazer do gateway para o alvo, ele não vai conseguir, pois o ArpON que está no *gateway* bloqueará, com isso, impedimos o ataque.

3.2.3.3 Dsniff

O Dsniff é um conjunto de ferramentas para testes de penetração e de auditoria numa rede, capaz de rastrear tráfego dos protocolos SMTP, FTP, TELNET, POP, SMB e pegar senhas de banco de dados SQL (ULBRICH, 2004).

Esta ferramenta é dividida em ferramentas passivas de monitoramento do tráfego na rede, ferramentas para intercepção de tráfego por parte de um atacante e ferramentas para implementação de ataques contra sessões SSH e HTTPS.

51 *Gateway* - É o equipamento que interliga duas redes que utilizam protocolos diferentes (MORIMOTO, 2005).

4 FERRAMENTAS DE DEFESA

Neste tópico estudaremos algumas ferramentas de prevenção e detecção de ataques para a segurança de uma rede, mostrando suas utilidades e funcionalidades, sem esquecer de ressaltar suas vantagens e desvantagens.

4.1 ANTIVÍRUS

É um programa de computador que detecta, evita e atua na neutralização ou remoção de programas mal-intencionados, como vírus e *worms* (MICROSOFT, 2012).

Segundo Kaspersky (2012), o vírus pode ser verificado por análise de assinaturas, usando bancos de dados que contêm as descrições de todos os *malwares* conhecidos e os métodos de desinfecção correspondentes, e por análise heurística, a qual analisa a estrutura de um arquivo, permitindo detectar incidências de novos vírus ou uma nova modificação de vírus conhecidos.

4.2 FIREWALL

É uma solução de segurança baseada em *hardware* ou *software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas (ALECRIM, 2013). A sua missão consiste basicamente em bloquear tráfego de dados indesejado e liberar acesso de acordo com suas políticas de segurança.

Conforme ALECRIM (2013), o Firewall é parte da segurança, mas não a segurança em si, então é necessário utilizá-lo com outra solução, de acordo com a estrutura da rede, necessidade especifica do que deve ser protegido e estratégias da organização.

Os *firewalls* são classificados em:

4.2.1 Packet Filtering

Um *firewall* de filtro de pacotes utiliza uma lista de regras de aceitação e/ou negação, as quais explicitamente definem os pacotes que serão admitidos pela interface de rede, e para isso examinam informação presente nos cabeçalhos dos pacotes. Após esta análise o pacote ou é enviado para o seu destino, ou silenciosamente descartado (rejeitado), ou bloqueado e enviado um pacote com condição de erro para a máquina remetente (negado) (FORTUNA, 2002).

É uma metodologia mais simples, uma vez que atua nas camadas de rede e transporte do modelo TCP/IP, examinando somente o cabeçalho dos pacotes (ALECRIM, 2013). A figura 5 mostra a metodologia deste tipo de *firewall*.

Por mais que seja uma das funções principais de um *Firewall*, a filtragem de pacotes usada desta forma não é o suficiente para garantir a segurança na rede, ele é apenas uma parte do conjunto, um componente do esquema global de segurança.

Figura 6 – *Stateless Firewall*
Fonte: ALECRIM, 2013.

A principal desvantagem desse tipo de tecnologia para a segurança reside na falta de controle de estado do pacote, o que permite que agentes maliciosos possam

produzir pacotes com endereço IP falsificado (IP *Spoofing*), segundo Jcvirtual (2012). Para resolver este problema, foi criado o *statefull firewall*, conforme estudaremos no tópico a seguir.

4.2.2 Statefull Firewall

Esta tecnologia permite ao *firewall* identificar o protocolo dos pacotes transitados e prever as respostas legítimas. Para tanto, o firewall guarda o estado de todas as últimas transações efetuadas e inspeciona o tráfego para evitar pacotes ilegítimos (JCVIRTUAL, 2012).

Este tipo de *firewall* baseia fundamentalmente nas informações do cabeçalho dos protocolos da camada de transporte e não filtra pacotes de forma isolada, mas sim com base em informações sobre o estado de conexões pré-estabelecidas (ALECRIM, 2013). A comunicação bidirecional é implícita, de forma que não há necessidade de se escrever regras de filtragem para cada um dos sentidos.

Um exemplo de *firewall statefull* mais utilizado atualmente é o Iptables, que permite editar a tabela de filtragem de pacotes, analisando o cabeçalho dos pacotes e, assim, tomar decisões sobre os destinos destes pacotes, considerando seus estados.

4.2.3 Firewall de Aplicação ou Proxy de Serviços

É um *firewall statefull* capaz de inspecionar os dados da camada de aplicação para tomar decisões mais inteligentes sobre a conexão.

Este tipo de *firewall*, que atua como intermediário entre um computador, ou uma rede interna, e outra rede externa, trabalha recebendo o fluxo de conexão, tratando as requisições como se fosse uma aplicação e originando um novo

pedido para o servidor de destino. (ALECRIM, 2013). A resposta para o pedido é recebida pelo *firewall* e analisada antes de ser entregue para o solicitante original.

A figura a seguir ajuda a compreender o conceito, uma vez que a rede interna não se comunica diretamente com a internet. Segundo Alecrim (2013), estes equipamentos ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber estes dados, acabam escondendo a identidade dos usuários e oferecendo uma proteção adicional contra a ação dos *hackers*.

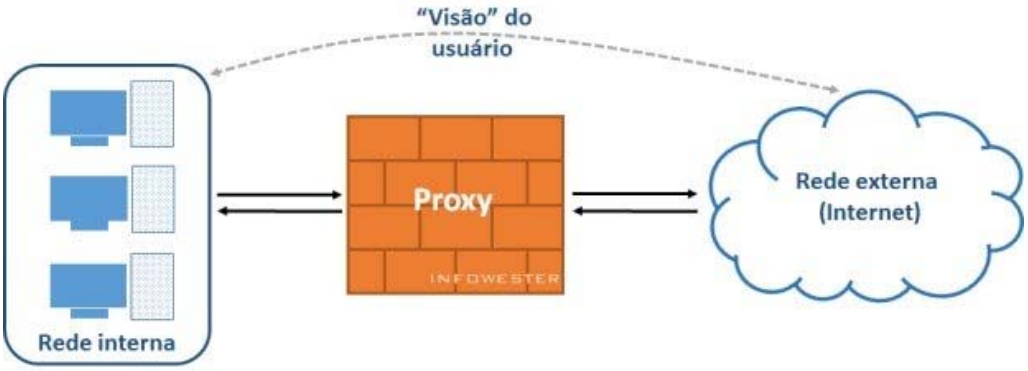


Figura 7 - Firewall de aplicação
Fonte: ALECRIM, 2013.

Todo o fluxo de dados necessita passar pelo p*roxy*, então é possível estabelecer regras que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre computadores internos e determinados serviços remotos.

Este controle amplo também possibilita o uso do *proxy* para tarefas complementares, como registrar o tráfego de dados em um arquivo de *log* e guardar temporariamente uma página *Web*, fazendo com que não seja necessário requisitá-la no endereço original a todo instante (ALECRIM, 2013).

Percebemos que *firewall* de aplicação possui algumas desvantagens, uma vez que introduzem perda de desempenho na rede, já que as mensagens devem ser processadas pelo agente do *Proxy*; exige manutenção especifica na aplicação de correções e na configuração dos servidores para manter um nível de segurança adequado; e fica vulnerável temporariamente a cada novo serviço que aparece na internet, sendo necessário o fabricante desenvolver um agente de *Proxy* correspondente (MACEDO, 2012).

4.3 SISTEMA DE DETECÇÃO DE INTRUSOS (IDS)

Sistema de detecção de intrusos[52] é um dos elementos essenciais à infraestrutura de segurança, cuja função é monitorar uma rede ou um host a procura de sinais padrões de comportamento que sejam considerados maliciosos, ou seja, que podem constituir um ataque de invasão ao sistema ou até menos algum usuário legítimo fazendo mau uso do mesmo. Da mesma forma, podem auxiliar os administradores na recuperação de danos, na identificação e no rastreamento de ações do atacante.

Em um sistema passivo, o IDS detecta uma potencial violação da segurança, registra a informação e dispara um alerta. Em um sistema reativo, o IDS responde à atividade suspeita, finalizando a sessão de usuário ou reprogramando o *Firewall* para bloquear o tráfego de rede da fonte maliciosa suspeita.

O IDS é muito útil como complementos aos mecanismos preventivos, detectando intrusões, gerando alertas, acionando contramedidas sempre que as propriedades de segurança dos sistemas de informação estiverem sob ataque e

[52] Intrusão - É qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou do sistema (HEADY, LUGER et al, 1990).

auxiliando na análise complexa de *logs*[53], que é a maneira mais comum para descobrir indícios de anomalias, tanto em hosts como no tráfego de rede (GASPAR; JESUS; SILVA, 2008).

Em contrapartida, existem situações indesejáveis que podem ocorrer em mecanismos de detecção de intrusão, cuja probabilidade de ocorrência pode induzir a erros, como a grande ocorrência de falso positivo[54] e falso negativo[55], sendo estes últimos os mais perigosos, pois podem aparentar uma falsa ideia de segurança.

A segmentação de redes por meio de switches, redes com altas taxas de transmissão e serviços criptografados (VPN, SSL e SSH), são fatores limitantes da atuação das ferramentas de detecção de intrusos, uma vez que dificultam a captura e análise dos pacotes que estão transitando na interface e, consequentemente, muitos ataques podem passar despercebidos (GASPAR; JESUS; SILVA, 2008).

Quanto ao funcionamento existem dois tipos de IDS, os baseados em sistemas de regras (*Rule-based Systems*) que usam da base de dados, onde fica todo e qualquer tipo de assinatura dos ataques, e do tipo Sistema Adaptável (baseado em anomalia) que possuem técnicas mais avançadas usando desde inteligência artificial até conhecimentos matemáticos e estatísticos (BORGES; BENTO, 2006).

A arquitetura de um IDS, quanto à natureza do alvo a ser monitorado, pode ser baseada em host, rede ou híbrido, conforme abaixo exposto:

---

[53] *Log* – É o registro de atividade gerado por programas e serviços de um computador (CERT.BR, 2013b).

[54] Falso Positivo – É a situação em que um IDS aponta uma atividade como sendo um ataque quando na verdade não é. Basicamente, um falso positivo é um alarme falso (GASPAR; JESUS; SILVA, 2008).

[55] Falso negativo - Ocorre quando alguém compromete um sistema monitorado por um IDS e este não gera alertas para atividades quedeveriam ser classificadas como sendo a do comportamento de um ataque (GASPAR; JESUS; SILVA, 2008).

4.3.1 Baseado em host (HIDS)

Possui um funcionamento bem simples de ser implementado e configurado, utilizando os dados coletados na própria máquina, como arquivos de *log*, registros de auditoria, integridade do sistema de arquivos, permitindo a determinação exata de quais usuários e processos estão realizando operações maliciosas no sistema.

Normalmente são instalados nos servidores críticos, tais como o DNS, *Webserver* e servidor de *e-mail*, e o que não for detectado pelo NIDS, será detectado nos HIDS instalados nestes servidores.

Segundo Bace e Melli (2004), as grandes vantagens dos HIDS é a menor probabilidade de ser descoberto em um eventual ataque e, além disso, ele pode operar em ambientes onde haja tráfego criptografado. No entanto, algumas desvantagens, como a dificuldade de gerenciamento, a perda de desempenho, devido ao alto consumo dos recursos computacionais e a impossibilidade de detecção dos ataques destinados à rede local, pois monitora apenas os pacotes recebidos pelo próprio host.

4.3.2 Baseado em rede (NIDS)

Este tipo de IDS é bem mais comum e utilizado. Eles realizam a monitoração do sistema por meio da captura e análise de cabeçalhos e conteúdo de pacotes de rede, os quais podem ser comparados com padrões de ataques conhecidos ou assinaturas previamente armazenadas em regras, arquivos ou bancos de dados, ou com padrões normais do tráfego, para verificação de algum desvio do comportamento normal da rede.

As grandes vantagens desse modelo é a sua implementação, uma vez que não afeta o funcionamento normal da rede, pois atua passivamente na escuta do

tráfego, por meio de um conjunto de sensores instalados em vários pontos da rede, realizando assim uma análise local e reportando ataques ao servidor. Com isso se bem posicionados podem monitorar uma grande rede, além de serem invisíveis a muitos atacantes (BACE; MELL, 2004).

Segundo Bace e Mell (2004), as desvantagens deste modelo é a grande dificuldade de processar todos os pacotes da rede, se eles forem grandes ou se a rede estiver congestionada, então o *firewall* pode não reconhecer um ataque em horários de pico, e a incapacidade de analisar informações criptografadas.

4.3.3 IDS Híbrido

Grande parte das ferramentas atuais de detecção de intrusão explora o melhor das arquiteturas baseadas em host e rede, adotando soluções híbridas.

Em busca de equilíbrio entre desempenho, simplicidade, abrangência e robustez, algumas implementações recentes provêm coleta de diferentes dados de hosts e do tráfego de rede, e interagem mecanismos centralizados com distribuídos.

4.4 SISTEMA DE PREVENÇÃO DE INTRUSOS (IPS)

É uma solução ativa de segurança com a capacidade para fornecer segurança em todos os níveis de sistemas, desde o núcleo do sistema operacional até os pacotes de dados da rede, por meio de políticas e regras para o tráfego de rede e, assim, emitir alertas em caso de tráfego suspeito, mas permite também que administradores executem ações relacionadas ao alerta dado (MORAES, 2012).

Enquanto o IDS informa sobre um potencial ataque, o IPS promove tentativas de parar o ataque. Ele precisa ser menos sensível que o IDS, porque ele molda o tráfego, em vez de apenas observá-lo.

Outro grande avanço sobre o IDS é que o IPS tem a capacidade de prevenir invasões com assinaturas conhecidas, mas também pode impedir alguns ataques não conhecidos, devido a sua base de dados de comportamento de ataques genéricos. Visto como uma combinação de IDS e de uma camada de aplicação do *Firewall* para proteção, o IPS geralmente é considerado a geração seguinte do IDS (UFRJ, 2010).

O ponto muito discutido deste tema é o posicionamento do IPS na topologia de rede, o qual tem gerado divergência entre os estudiosos deste assunto. Na primeira parte da figura 8, apenas o tráfego permitido pelo *firewall* é passado ao IPS, o qual, por sua vez, tem função de promover uma inspeção mais detalhada. Enquanto, no segundo modelo, todos os pacotes passariam inicialmente pelo IPS antes de chegar à interface *outside* do firewall (MORAES, 2012).

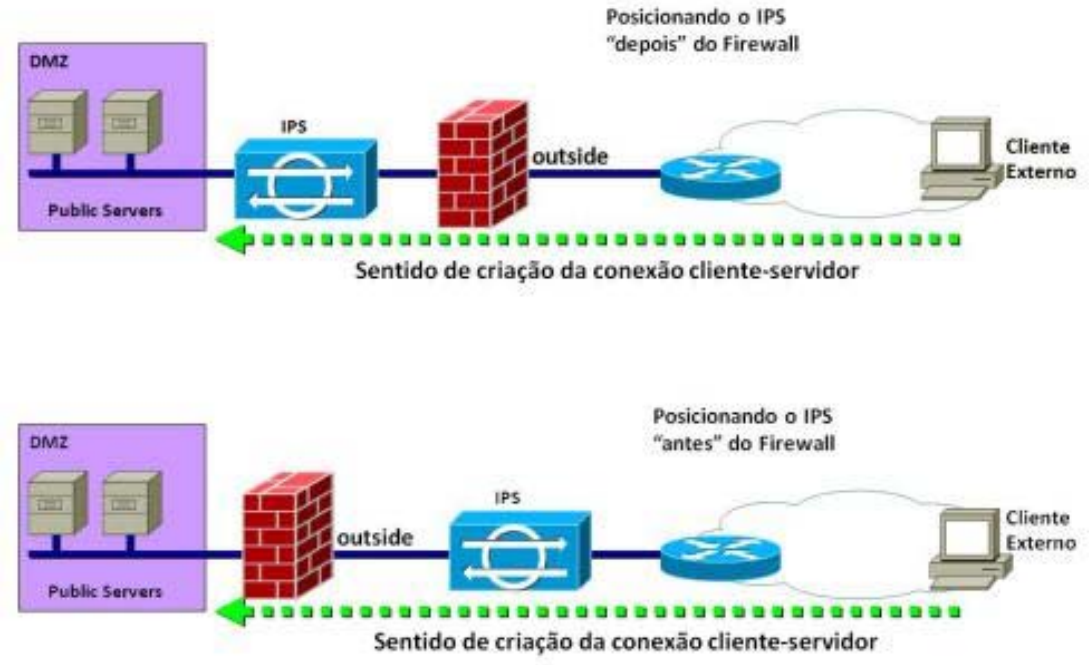


Figura 8 – Posicionamento do IPS
Fonte: MORAES, 2012.

O modelo que emprega o IPS após o *firewall* é mais adequado tanto em projetos em que os equipamentos são distintos quanto naqueles em que o IPS consiste em um módulo do *firewall*. Na segunda opção é ainda comum que o *firewall* selecione os tipos de tráfego que serão direcionados ao IPS, em vez de se fazer o espelhamento completo, ação esta que também contribui para um melhor uso dos recursos de IPS.

4.5 SECUTITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Enquanto o volume de informações e o número de ameaças continuam a crescer, os sistemas tradicionais de gerenciamento de *log* não podem lidar com grandes volumes de dados de segurança. Diante disso, existem tecnologias comprovadas capazes de ajudar e a atual geração de SI e gestão de eventos (SIEM) é um excelente exemplo.

Segundo Clm ([201-?]), SIEM é um conceito relativamente novo que surgiu em 1999 e evolui gradativamente com novas funções, fornecendo uma análise em tempo real de alertas de segurança gerados por *hardware* e aplicativos de rede.

Este conceito foca na capacidade de capturar, analisar, apresentar informações de rede e dispositivos de segurança, em identificar e acessar aplicativos de gerenciamento, em ferramentas de gerenciamento de vulnerabilidades e política de conformidade, em sistemas operacionais, *logs* de banco de dados e de aplicativos, e em dados sobre ameaças externas (MCAFEE, 2014).

As principais áreas de atuação incluem o monitoramento e gerenciamento de usuários e privilégios de serviço, serviços de diretório e outras alterações de configuração do sistema, bem como o fornecimento de auditoria e resposta à incidentes.

O objetivo das soluções SIEM é precisamente comparar, em um único local, todos os dados coletados por uma variedade de dispositivos de segurança, aplicações e fontes de dados, sendo possível reunir os roteadores, switches e máquinas virtuais e depois normalizar os dados (MCAFEE, 2014), conforme mostrado na figura 9. Como resultado, é possível, por exemplo, ver o que um endereço IP fez em todos os *firewalls* de uma organização, possibilitando o rastreamento das atividades para uma análise posterior detalhada.

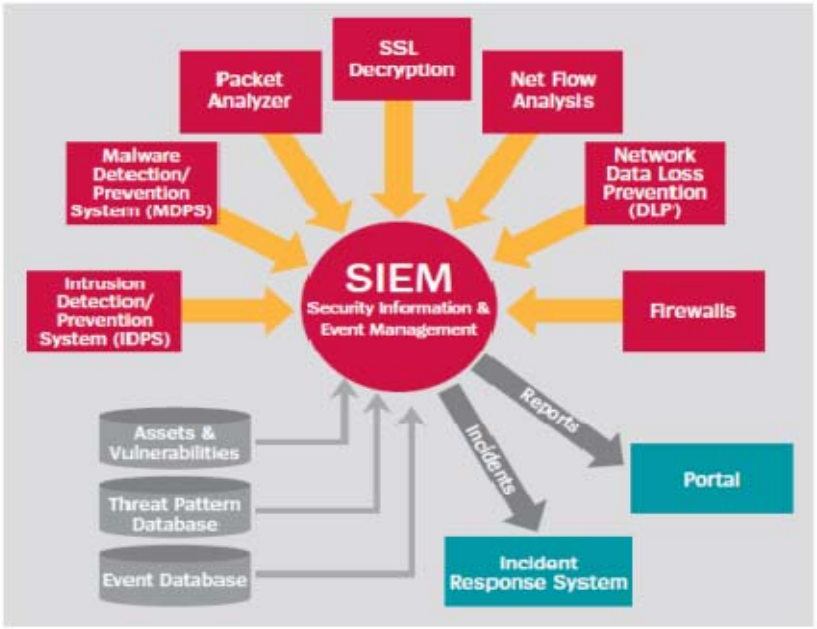


Figura 9 - SIEM
Fonte: UNISYS, 2014.

4.6 REDE VIRTUAL PRIVADA (VPN)

As redes públicas são consideradas não confiáveis, uma vez que os dados trafegados na rede estão sujeitos à interceptação e captura. Diante da necessidade de transmissão de dados de forma confiável, surgiu o conceito de VPN (FRANZIN; ROSSI, 2000).

As VPN são redes que possibilitam um acesso privado de comunicação, por meio da rede publica já existente, como a internet, assegurando a comunicação entre dois pontos por meio de um túnel onde os dados ficam inacessíveis à escutas clandestinas e interferência.

Par garantir a comunicação segura, as VPN proveem um conjunto de funções que garantam a confidencialidade, integridade e autenticidade e possuem seus próprios protocolos de comunicação, como por exemplo o IPSEC[56], que atuam em conjunto com o TCP/IP, fazendo com que o túnel virtual seja estabelecido e os dados trafeguem criptografados (FRANZIN; ROSSI, 2000).

4.7 WEB APLICATION FIREWALL (WAF)

Nos últimos anos, as aplicações *web* cada vez mais tem se tornado alvo de ataques de *hackers*, os quais estão explorando os potenciais pontos fracos no próprio *software* de aplicações *web*. Para se defender deste tipo de ataque surgiu o WAF.

O *firewall* de aplicação *web* é uma tecnologia de SI em evolução projetada para proteger aplicações *web* contra ataques, em que os firewalls de rede e IDS não conseguem impedir, aumentando a confiabilidade, integridade e disponibilidade do *website*, segundo Exceda ([201-?]).

Ele emite alertas e realiza bloqueios, filtrando todo o trafego HTTP e HTTPS de entrada, por meio de controles configuráveis nas camadas de rede e aplicação,

[56] IPSEC (Internet Protocol Security) - É um conjunto de protocolos que oferece segurança para comunicações via Internet na camada IP. Sua função é fornecer uma Virtual Private Network (VPN) entre dois locais (gateway-to-gateway), entre um usuário remoto e uma rede corporativa (host-to-gateway), ou host-to-host. (RFC 6071, 2011).

da mesma forma que detecta e previne técnicas de exploração comuns, como SQL *Injection*[57] e *Cross Site Scripting* (XSS) [58] (OWASP, 2014).

Segundo Owasp (2008), além da função de proteção, o WAF torna-se um ponto de serviço central para realização de tarefas que podem e devem ser tratados da mesma forma para todas as aplicações, implementando tarefas que podem ser resolvidas da mesma maneira para cada aplicação. Como por exemplo o monitoramento, elaboração de relatórios e processo de localização de erro, que são consideravelmente simplificados, quando avaliados centralmente no WAF.

4.8 DATA LOST PREVENTION (DLP)

Com o aumento da complexidade no uso e compartilhamento da informação, surgiu a necessidade de que a confidencialidade, integridade e disponibilidade deste dado seja garantida. Para isso, surgiu uma nova abordagem para proteção dos dados contra problemas vindos de dentro ou de fora da organização, armazenados ou trafegando na rede, em servidores centrais ou em computadores pessoais.

O termo Data Loss Prevention (DLP) é utilizado na área de SID para se referir a sistemas e metodologias que possibilitam as empresas reduzir o risco do vazamento de informações confidenciais. Os sistemas DLPs podem identificar a perda de dados através da identificação do conteúdo, monitoramento e bloqueio de dados sensíveis, ou seja, identificar, monitorar e proteger as informações confidencias que podem estar em uso (máquinas dos usuários), em movimento (na

[57] SQL *Injection* - É um ataque de injeção de comando SQL em campos de entrada de dados em uma aplicação, permitindo ler, modificar dados sensíveis do banco de dados e executar operações de administração do banco de dados (OWASP, 2013).
[58] *Cross Site Scripting* (XSS) - Consiste em uma vulnerabilidade causada pela falha nas validações dos parâmetros de entrada do usuário e na resposta do servidor em uma aplicação web, permitindo que códigos maliciosos sejam executados no navegador do usuário (VIEIRA, 2008).

rede corporativa) ou armazenadas (banco de dados e servidores) (FERREIRA, 2012).

Como o conceito ainda é novo, então ainda há muitos nomes. Segundo Bezerra (2008), alguns autores chamam de *data loss prevention* (prevenção de perda de dados), outros usam a mesma sigla DLP, mas com uma pequena diferença, *Data Leakage Prevention* (prevenção de vazamento de dados). Há ainda uma corrente chamando de *data-centric security* (segurança centrada em dados). Apesar dos múltiplos nomes, o DLP é um processo constante de conhecer, classificar, proteger e monitorar os dados, estejam eles onde estiverem.

O DLP define e gerencia políticas de proteção dos dados para toda a organização, não se preocupando com a proteção da infraestrutura. O foco está no dado que viaja e descansa dentro da infraestrutura e no seu ciclo de vida (FERREIRA, 2012).

Com a inclusão deste novo conceito, foi possível a aproximação das equipes de proteção com as áreas de negócio da organização, permitindo identificar os processos de negócios falhos que estejam transmitindo dados confidenciais.

4.9 ANTI-DDOS

É uma ferramenta de segurança desenvolvida para a detecção e eliminação de ataques do tipo DoS, DDoS e DRDOS, utilizando a análise comportamental, assinaturas de tráfego, limitação de taxa e outras técnicas para identificar e bloquear o tráfego malicioso (NETWORK BOX, 2013).

Esta ferramenta de proteção multi-camada bloqueia ataques de *flood* de rede e camada de aplicação[59], onde a taxa de conexão, o volume de transferência de dados e conexão lenta podem ser tratadas, e as propriedades da camada 7 (OSI), incluindo padrão de URL, agente de usuário e cabeçalho da solicitação são levados em consideração, conforme mostrado na figura 10.

Para tanto, é utilizado *whitelists*[60] e *blacklists*[61] de endereços IP e uma vez que a origem dos ataques foi identificada, ela é adicionada à lista negra, e o tráfego a partir desta fonte é bloqueado por um tempo determinado ou indefinidamente.

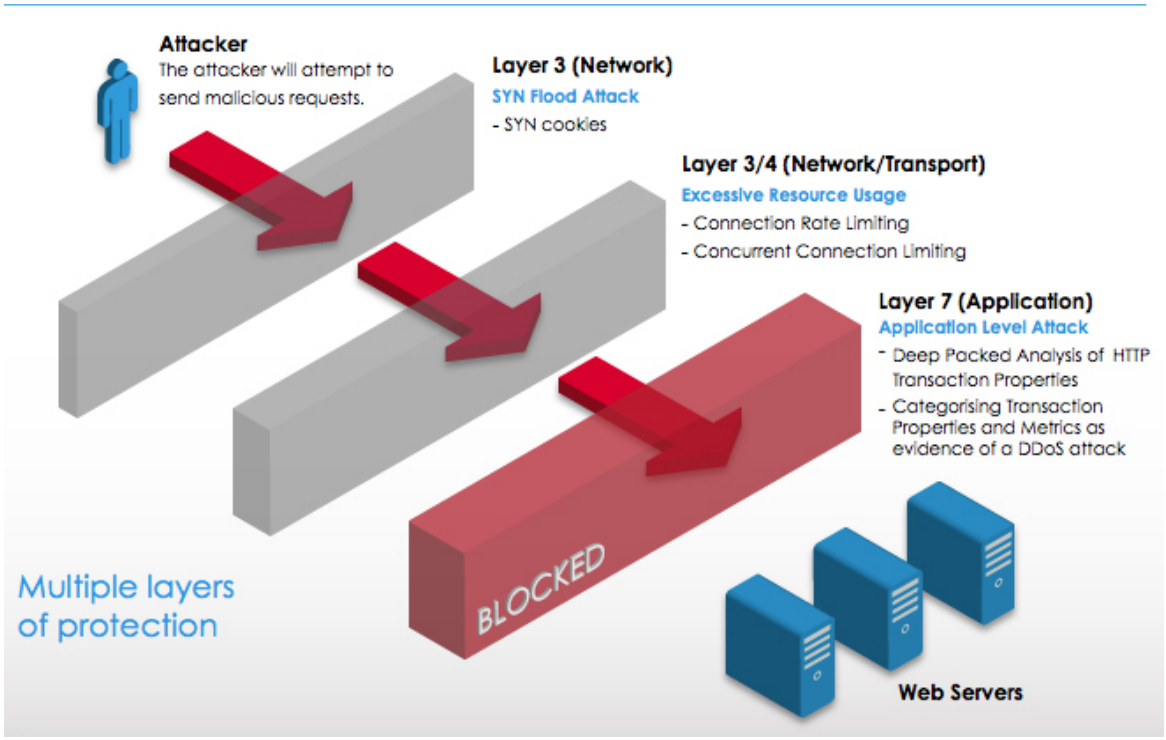


Figura 10 - Anti–DDoS
Fonte: NETWORK BOX, 2013.

[59] Camada de Aplicação (Camada 7 OSI) – Esta camada serve como a janela onde os processos de aplicativos e usuários podem acessar serviços de rede (MICROSOFT, 2013).
[60] *Whitelists* - Trata-se de uma lista de endereços IP, previamente aprovados e que, normalmente, não são submetidos aos filtros anti-DDoS configurados (UFES, 2014).
[61] *Blacklist* - Trata-se de uma lista de endereços IP reconhecidamente fontes de DDoS. Geralmente, utiliza-se este recurso para bloquear os IPs suspeitos de serem origem de ataques (UFES, 2014).

5 ABORDAGEM INTEGRADA

Como resultado do avanço da comunicação móvel e a computação em nuvem, as organizações enfrentam desafios para manter seus dados e sistemas seguros e ter o controle completo sobre a infraestrutura da rede, então elas precisam escolher em ter um único console de gerenciamento (abordagem tradicional) ou optar por um modelo de segurança integrada.

Atualmente, o modelo tradicional de segurança, o *firewall* de primeira geração, não é capaz de identificar as novas variações de *malware* e ataques do mundo cibernético, deixando as organizações extremamente vulneráveis às novas ameaças.

Para isso neste trabalho analisaremos a adoção de diferentes controles e mecanismos de proteção integrados em diferentes níveis, implantando uma arquitetura de defesa em profundidade.

5.1 MODELO DE CAMADAS DA DEFESA EM PROFUNDIDADE

É uma estratégia adotada pela SI que consiste no uso de várias camadas de proteção para os dados, evitando o acesso direto a eles por um usuário ou sistema. Esta estratégia permite endereçar problemas de segurança inerentes às pessoas, processos e tecnologia, durante o ciclo de vida útil da informação (MICROSOFT, 2011). A figura 10 demonstra este conceito.

Segundo Horton (2003), as organizações devem empregar um modelo de abordagem de defesa em camadas, possibilitando alcançar uma segurança maior e as exigências de conformidade com as normas, prevenindo ou detectando estes novos ataques e estratégias de penetração persistentes por meio de múltiplos, redundantes e independentes níveis de proteção.

Figura 11 - Defesa em Profundidade.
Fonte: SALVATORE, 2012.

A defesa em camadas baseia-se em mecanismos e controles para tornar a rede mais segura, através de meios técnicos e operacionais que a organização pode utilizar para proteger seus bens e informações e cuja finalidade é detectar falhas de segurança, reagir e recuperar esses bens e informações (HORSON, 2003). E são estes mecanismos, como *firewall*, VPN, IPS, IDS, certificação digital que atenderão às regras especificadas na política de segurança.

Enquanto isso, uma política de segurança tem o propósito de regular como deve ser gerenciada e protegida a informação, além dos recursos e usuários, que com ela interagem durante todo o seu ciclo de vida, fornecendo orientação e apoio às ações de gestão de segurança (VAZ, [201-?]). Para isso, pode ser usado controle de acesso e serviço de monitoramento com câmeras e alarmes.

Ao combinar vários mecanismos de proteção, é implementado camadas de segurança com objetivos e intensidades diferentes, variando os tipos de controles

utilizados, visando desestimular ou dificultar o sucesso da ameaça desde o inicio de sua investida, e caso obtenha sucesso ao ultrapassar uma barreira, encontrará outras com estratégias diferentes para evitar que ela obtenha sucesso (VAZ, [201-?])

O presente trabalho sugere alguns pontos importantes da defesa em profundidade, a fim de podermos encontrar um equilíbrio para manter um ambiente extremamente seguro sem sobrecarregar a estrutura de TI da organização e sem afetar o desempenho das aplicações.

1) Os aspectos de segurança dos aplicativos devem ser verificados no processo de desenvolvimento e homologação, por meio de testes de qualidade e segurança. Para isso há a necessidade de treinamento do pessoal envolvido com o desenvolvimento e o investimento em ferramentas de testes para encontrar erros e vulnerabilidades em *softwares*, reduzindo o tempo gasto para mitigar os pontos fracos do desenvolvimento.

2) É necessário um reforço na defesa da borda da rede, começando com o robustecimento das tecnologias de segurança, a fim de dificultar ataques externos, uma vez que tem o maior trafego de dados e não pode degradar o desempenho da rede. Para tanto, podemos usar o IPS e IDS juntos, fazer a análise do comportamento da rede e monitoração de DDOS, *fiwerall*, *antivirus*, *WAF* e Anti-*Spam*, conforme detalhado no capitulo 4, a fim de detectarmos e bloquearmos possíveis ataques em todos os níveis.

Da mesma forma, ter pontos de estrangulamento na rede é uma das principais estratégias de proteção, uma vez que quanto menos entradas a rede tiver, mais fácil

é o processo de monitorá-las e torná-las seguras, utilizando os equipamentos citados anteriormente (SILVA, 2011b).

3) Nas camadas interiores, podemos usar o UTM (*Unified Threat Management*), o qual é uma solução que tem a capacidade de executar várias funções de segurança num único dispositivo: *firewall*, prevenção de intrusões de rede, *antivírus*, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede (BLUEPEX, [201-?]), facilitando a administração e permitindo pessoal menos capacitado dar suporte à rede.

4) Quando um ataque passa pelas defesas de borda da rede, as estações de trabalho e servidores devem estar prontos para bloqueá-lo ou minimizar os danos.

Os produtos de proteção individual, como *Antívirus* e *Firewal*l Pessoal, podem ser integrados em plataformas de gerenciamento centralizado, facilitando a administração e proporcionam uma proteção equivalente, com custos menores que a utilização das ferramentas de forma separada.

5) A falta de gerenciamento dos ativos e das informações da organização pode torná-la vulnerável à ataques cibernéticos ou à roubo/vazamento de informações. Segundo Salvatore (2012), diante disso há a necessidade implementar soluções de gerenciamento de governança[62], chamado MSS (*Managed Security Services*), que permite conhecer as vulnerabilidades existentes em todos os aplicativos utilizados e no sistema operacional.

[62] Governança - é o conjunto formado pela cultura, as políticas, os processos, as leis e as instituições que definem a estrutura segundo a qual as empresas são comandadas e administradas (SANCHES, 2008).

Da mesma forma, implantar o GRC (*Governance Risk Management and Compliance*), o qual engloba as áreas de governança, risco[63] e *compliance*[64] atuando em conjunto, estabelecendo uma postura proativa capaz de prevenir a incidência de eventos de risco e violações de conformidade.

6) A segurança na comunicação também é muito importante para garantir a confidencialidade, a integridade e a autenticidade dos dados trafegados. Para isso podemos usar uma VPN para garantir uma conexão segura em uma infraestrutura pública, conforme mencionado no item 4.5.

7) A segurança de um sistema é igual à segurança de seu dispositivo mais frágil e os usuários são considerados o elo mais fraco da estrutura, pois seriam os elementos mais susceptíveis a manipulação e mais difíceis de controlar (SILVA, 2011b).

Precisamos garantir que usuários autorizados não sejam indevidamente atrapalhados por requisitos de segurança excessivos, enquanto as pessoas não autorizadas sejam devidamente bloqueadas. Para isso precisamos ter políticas de segurança bem definidas com a Identificação e gerenciamento de acesso de usuários.

Para a proteção dos dados moveis e armazenados, podemos utilizar criptografia, estabelecer rotinas de *backup* e recuperação, e realizar monitoramento de conteúdo e prevenção de vazamentos (DLP), uma vez que só as tecnologias são incapazes

[63] Risco – é o efeito das incertezas nos objetivos. É relacionado à probabilidade de um evento ocorrer e aos possíveis impactos do evento nos objetivos de negócio (SANCHES, 2008).
[64] Compliance - consiste em aderir às leis e outras formas de regulamentações, assim como em tornar explícita esta adesão, tanto com relação a leis e regulamentações externas quanto a políticas e procedimentos corporativos (SANCHES, 2008).

de proteger o dado das novas técnicas e métodos de ataque. Esta nova abordagem de segurança DLP foi detalhada no item 4.7.

Da mesma forma, é importante a realização periódica de treinamentos e campanhas de conscientização específicas na área de segurança da informação, a fim de que seja estimulada uma mentalidade nos usuários voltada para esta área.

8) Caso o ataque seja bem sucedido, devemos nos preocupar em ter ferramentas de gerencia de segurança, a fim de verificar os rastros do atacante, por meio do gerenciamento de eventos e *logs*, avaliar o ataque e os vazamentos, utilizando forense digital e ativar o plano de continuidade do negócio, evitando que os processos críticos do negócio da organização sejam afetados (SALVATORE, 2012).

O desafio não é somente proteger os dados, mas fazer isso de maneira a permitir que as aplicações mantenham a escalabilidade, o desempenho e permaneçam altamente disponíveis.

6 CONCLUSÃO

Diante da total dependência dos sistemas computacionais e da internet, a sociedade moderna tem observado o aumento dos casos de ataques cibernéticos ocorridos na última década, como os casos Stuxnet e da Estonia, levando os governos de alguns países a iniciarem ações para proteger suas infraestruturas críticas dos possíveis ataques no espaço cibernético.

A guerra cibernética é a nova frente de batalha em um mundo marcado pela interdependência e pela crescente complexidade tecnológica. Diante desta nova modalidade de guerra, este trabalho nos permitiu analisar os casos mais importantes de ataques no ciberespaço, bem como os métodos, as técnicas e as ferramentas utilizadas. Da mesma forma, estudamos o outro lado desta batalha assimétrica, visualizando as ferramentas e equipamentos que podem ser usados para defender os ativos de informação que afetam diretamente a missão do País e a segurança da sociedade.

Por fim foi introduzido o conceito de defesa em profundidade, onde no cenário atual de ameaças em rápida evolução, proteger a rede somente com um *firewall* não é o suficiente. As organizações exigem cada vez mais uma abordagem de defesa em profundidade, onde diversas camadas e serviços de segurança trabalham de forma cooperativa para detectar, bloquear e relatar dinamicamente a existência de tráfego mal-intencionado, sem deixar de permitir a passagem do tráfego normal com a maior eficiência possível.

No Brasil, as vulnerabilidades de um conjunto complexo de redes informatizadas, a pouca cultura em segurança da informação e comunicações e o apoio tímido da alta administração, são alguns fatores que justificam o resultado de um estudo divulgado recentemente pela empresa de *antivírus* McAfee e produzido

pelo centro de pesquisas belga Security Defense Agenda (SDA), o qual apontou que o Brasil é dos países menos preparados para ataques cibernéticos em um *ranking* de 23 nações. Segundo Mandarino (2012), isto se deve ao fato do País não estar envolvido em guerras e por isso o espaço cibernético não é visto como um campo de batalhas.

A falta de uma legislação especifica para combater crimes cibernéticos é o nosso ponto fraco e o assunto segurança e defesa do espaço cibernético ainda não despertou a atenção que merece, nem mesmo no meio militar.

Ainda estamos iniciando neste assunto, então para minimizar os possíveis impactos da falta de regras especificas para delimitar ações no ciberespaço, é necessário realizar medidas preventivas conjuntas entre os órgãos da Administração Pública Federal (APF) e as Forças Armadas (FFAA), com o apoio do governo na construção de uma Estratégia de Segurança Cibernética simples e escalável, a fim de adotar uma postura rígida de defesa e, com isso, garantir a segurança do sistema cibernético no País.

Da mesma forma, precisamos promover uma mudança de cultura, colocando a SI como atividade estratégica do País, priorizando investimentos em tecnologia e recursos humanos, bem como conscientizar a sociedade sobre a importância deste tema, realizar acordos internacionais para compartilhamento de experiências, a fim de criar um processo contínuo que substitua as ações pontuais.

REFERÊNCIAS

AARON. *CCNP Switch 642-813 - Spoofing Attacks*, 2010. Disponível em: <http://www. ccnpguide.com/ccnp-switch-642-813-spoofing-attacks/>. Acesso em: 27 fev. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 6023*: Informação e documentação. Referências: elaboração. Rio de Janeiro, ago. 2002. 24p.

_____. *NBR 10520*: Informação e documentação. Citações em documentos: apresentação. Rio de Janeiro, ago. 2002. 7p.

_____. *NBR 14724*: Informação e documentação. Trabalhos acadêmicos: apresentação. Rio de Janeiro, mar. 2011. 11 p.

ALECRIM, *E. O que é firewall? - Conceito, tipos e arquiteturas*, 2013. Disponível em: <http://www. infowester.com/firewall.php>. Acesso em: 27 jan 2014.

ALECRIM, E. *O que é tecnologia da informação?*, 2011. Disponível em: <http://www.infowester.com/ ti.php>. Acesso em: 06 fev. 2014.

ALVES, C. B. *Segurança da informação vs. Engenharia Social - Como se proteger para não ser mais uma vítima*, 2010. Disponível em: <http://monografias.brasilescola.com/ computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm>. Acesso em: 06 fev. 2014.

ARAUJO, R. B. *Especificação e análise de um sistema distribuído de realidade virtual*. Tese (Doutorado) - Departamento de Engenharia de Computação e Sistemas Digitais. Escola Politécnica da Universidade de São Paulo, 1996. 144p.

BACE, R.; MELL, P. *NIST Special Publication on Intrusion Detection Sistems*, 2011. Disponível em <http:// cryptome.org/sp800-31.htm>. Acesso em: 07 fev.2014.

BEZERRA, M. Blog *Segurança Digital - Artigo sobre Guerra Cibernética "Cyberwar"*, [200-?]. Disponível em: <Http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq>. Acesso em: 03 dez. 2013.

BEZERRA, M. Data Loss Prevention, 2008. Disponível em: http:// segdigital.blogspot.com.br/2008/ 03/data-loss-prevention.html. Acesso em: 05 fev. 2014.

BOFF, C. Técnicas do Hackerismo, 2009. Disponível em: <http://www. batebyte. pr.gov.br/modules/conteudo/conteudo.php?conteudo=1212>. Acesso em: 20 jan. 2014.

BORGES, C. F. P; BENTO P. D. N. *Segurança de redes utilizando honeypots*. Monografia de Conclusão de Curso para obtenção do Grau de Engenharia da Computação apresentada ao Instituto de Estudos Superiores da Amazônia, 2006. Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/computacao/article/viewFile/83/78>. Acesso em: 22 jan. 2014.

BLUEPEX. *O que é UTM?,* [201-?]. Disponível em < http://www.bluepexutm.com/ site/_ por/o-que-e-utm/>. Acesso em: 15 fev. 2014.

BRADLEY, T. *Introduction to Port Scanning* – 2012. Disponível em: <http:// netsecurity.about.com/cs/ hackertools/a/aa121303.htm>. Acesso em: 20 jan. 2014.

BRASIL. *Manual MD30-M-01 - Doutrina de Operações Conjuntas*. v.2, 1.ed, p.54. Brasilia: Ministério da Defesa, 2011. Disponível em: < http://www.defesa.gov.br/ arquivos/File/legislacao/emcfa/ publicacoes/md_30_m_01_2volume.pdf. Acesso em: 11 jan. 2014.

BRASIL. *Manual MD35-G-01 - Glossário das Forças Armadas*. 4.ed, p.123. Brasilia: Ministério da Defesa 2007. Disponível em: <http://www.hmab.eb.mil.br/downloads/ outros/glossario_fa.pdf Acesso em: 11 jan. 2014.

BRASIL. *Manual de Campanha - C 34-01 - Emprego da Guerra Eletrônica*. 1.ed. Brasilia: Ministério da Defesa, 1999. Disponível em: <https://doutrina.ensino.eb.br/ Manuais/C%2034-1.pdf/>. Acesso em: 11 jan. 2014.

BROAD, W. J; MARKOFF, J.; SANGER, D. E. I. *Test on Worm Called Crucial in Iran Nuclear Delay*. Disponível em: <http://www.nytimes.com/2011/01/16/world/ middleeast/16stuxnet.html?pagewanted =1&_ r=1/>. Acesso em: 11 dez. 2013.

CERT.BR. *Incidentes reportado ao CERT.br de Julho a Setembro*, 2013a. Disponível em: <http://www.cert.br/stats/incidentes/2013-jul-sep/tipos-ataque.html>. Acesso em: 03 dez. 2013.

CERT.BR. *Cartilha de Segurança para internet – Parte II: Riscos Envolvidos no uso da internet e Métodos de prevenção*, 2013b. Disponível em: <http://cartilha. cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos. pdf>. Acesso em: 19 fev. 2014.

CAHILL, T. P.; ROZINOV, K.; MULÉ, C. *Cyber Warfare Peacekeeping Proceedings of the IEEE Workshop on Information Assurance.* West Point, NY, p 100–107, 2003. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2003, West Point, NY. Disponível em:<http://www.sige.ita.br/sige_old/IXSIGE/Artigos/GE_39.pdf>. Acesso em: 25 de fev. 2014.

CARNEGIE, M. *TCP SYN Flooding and IP Spoofing Attacks*, 2000. Disponível em:<http://www.cert. org/advisories/CA-1996-21.html>. Acesso em: 25 de jan. 2014.

CARVALHO, F. G. *Armas e sistemas de armamento de tecnologia avançada ou o "Aggiornamento" da "Arte da Guerra"*, 2012. Disponível em: <http://www.odiario. info/?p=2544>. Acesso em: 07 fev. 2014.

CÁSSIO B. A. *Segurança da Informação vs. Engenharia Social. Como se proteger para não ser mais uma vítima*, 2010. Monografia - Centro Universitário do Distrito Federal – UDF, Brasília, 2010. Disponível em: http://www.administradores.com.br/

_resources/files/_modules/academics/ academics_ 3635_20101207234707794d. pdf. Acesso em: 18 dez. 2013.

CASTILHO, C. *A diplomacia (ou guerra) da informação*, 2013. Disponível em: < http://observatoriodaimprensa.com.br/codigoaberto/post/a_diplomacia_ou_guerra_da _informacao>. Acesso em: 11 dez. 2013.

CLARK, R. A.; KNAKE, R. *Cyber War. The next threat to national security and what to do about it.* [s.l]:Haper colins, 2010. 320p

CLM. *SIEM – Security Information and Event Management*, [201-?]. Disponível em: <http://www.clm.com.br/solucoes/siem.htm>. Acesso em: 07 fev. 2014.

COMPUTERWORLD. *Kaspersky descobre linguagem usada em vírus Duqu* 2012. Disponível em: < http://www.computerworld.com.pt/2012/03/20/kaspersky-descobre-linguagem-usada-em-virus-duqu/>. Acesso em: 07 fev 2014.

DITTRICH, D. *The DoS Project's "trinoo" distributed denial of service attack tool*, 1999. Disponível em: <http://staff.washington.edu/dittrich/misc/trinoo.analysis>. Acesso em: 21 fev. 2014.

DUARTE, L. O. *Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x*, 2003. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação. São José do Rio Preto, SP. NESP/ IBILCE. 55p. Disponível em: <http://www.academia.edu/483738/Analise_ de_Vulnerabilidades_ e_Ataques_ Inerentes_a_Redes_Sem_Fio_802.11_x>. Acesso em: 21 jan. 2014.

DUNN, J. E. *Cibercriminosos mudam táticas em ataques DDoS, dizem pesquisadores*, 2013. Disponível em <http://www.tirio.org.br/cgi/cgilua.exe/sys/start. htm?infoid=29344&sid=118>. Acesso em: 05 fev. 2014.

EB. *Revista do Exercito Brasileiro*. Vol 149, 2013. Disponível em: <http://pt.calameo.com/read/ 001238206530442dcc28b>. Acesso em: 06 fev. 2014.

EXCEDA. *WAF Web Aplication Firewall*, [201-?]. Disponível em: <http://www. exceda.com/produtos/ waf-web-application-firewall/>. Acesso em: 05 fev. 2014.

FABIANO, C. *Spamhaus vítima de ataque de DDoS em larga escala*, 2013. Disponível em: <http://carlosfabiano.wordpress.com/ 2013/ 03/ 30/spamhaus-vitima-de-ataque-de-ddos-em-larga-escala/>. Acesso em: 05 fev. 2014.

FALLIRTE, N.; MURCHU, L. O.; CHIEN, E. *W32. Stuxnet Dossier. Symantec*, 2011. Disponível em: <http://www.wired.com/images_blogs/ threatlevel/ 2011/02/ Symantec-Stuxnet-Update-Feb-2011.pdf>. Acesso em: 13 jan. 2014.

FELTEN, E. W. et. al. *Web Spoofing: An Internet Con Game*, 1997. Disponível em: http://sip.cs. princeton.edu/pub/spoofing.html. Acesso em: 13 fev. 2014.

FERRAN, L. Bigger *Than flame, stronger than Stuxnet: why "idiot" humans are best Cyber Weapon*, 2012. Disponível em: <http://abcnews.go.com/ blogs/headlines/

2012/06/bigger- than- flame- stronger-than- stuxnet- why- idiot- humans-are- best-cyberweapon/>. Acesso em: 13 jan. 2014.

FERRAZO, G. M. *Entendendo como funcionam os ataques cibernéticos em massa – Parte 1 – Segurança Digital contra Ataques (DDOS E DRDOS),* 2011. DISPONÍVEL EM: <http://aghatha.wordpress.com/2011/07/10/entendendo-como-funcionam-os-ataques-ciberneticos-em-massa-tipo-ddos-e-drdos/>. Acesso em: 06 fev. 2014.

FERREIRA, M. *O que é Data Loss Prevention (DLP)?,* 2012. Disponível em: <http://www.security.blog.br/2012/04/o-que-e-data-loss-prevention-dlp/>. Acesso em: 05 fev. 2014.

FONTENELE, M. P. *Proposta de Taxionomia da Guerra de Informação e das Operações de Informação*, [2008?]. Disponível em: <http://www.ccomgex.eb.mil.br/cige/sent_colina/ 9_edicao_abr_10/index/Art_Maj_Fontenele.pdf/>. Acesso em: 26 nov. 2013.

FORTUNA, P. *Firewalls e Linux. Tutorial IpTables*, 2002. Instituto Superior de Engenharia do Porto. Projeto Final do Curso de Engenharia Informática. Disponível em: <http://www.dei.isep.ipp.pt/~paf/proj/Set2002/Firewall%20&%20Linux%20-%20 Tutorial%20de%20 iptables.pdf. Acesso em: 26 jan. 2014.

FRANZIN, M. A. ROSSI, O. *VPN (Virtual Private Network),* 2000. Disponível em: <http://www.gpr.com.br/download/vpn.pdf>. Acesso em: 04 fev. 2014.

GALLAGHER, S*. Researchers discover zero-day Windows exploit in Duqu virus* – 2011. Disponível em: <http://arstechnica.com/business/2011/11/researchers-discover-zero-daywindows-exploit-in-duqu-virus/>. Acesso em: 06 fev. 2014.

GALOSSI, R. *Entendendo o ataque ARP spoofing + SSLStrip*, 2013. Disponível em: <http://www.vivaolinux. com.br/artigo/Entendendo-o-ataque-ARP-spoofing-SSLStrip/>. Acesso em: 27 jan. 2014.

GASPAR, A. E. O.; JESUS, K. L. S.; SILVA, M. C. *Um estudo sobre sistema de detecção de intrusão*, 2008. Monografia de conclusão de curso apresentada no curso de Pós-Graduação em Suporte a Redes de Computadores e Tecnologia Internet do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará. Disponível em: <http:// pt.scribd.com/ doc/ 3752728/monografia-ids/>. Acesso em: 07 fev. 2014.

GUILHERME, P. *O que é ping?,* 2012. Disponível em: <http://www.tecmundo. com.br/internet/715-o-que-e-ping-.htm/>. Acesso em: 07 jan. 2014.

GRIS. *Flame: a nova ciberarma*, 2012. Disponível em: http://www.gris.dcc.ufrj.br/news/flame-nova-ciber-arma-parte-1/>. Acesso em: 18 fev. 2014.

HENRIQUE, P. Como *funciona o ataque DRDoS, o novo ataque de negação de serviço*, 2013. Disponível em: <http://www.inforedes.eti.br/2013/07/como-funciona-o-ataque-drdos-o-novo.html>. Acesso em: 05 fev. 2014.

HORTON, M. H. *Notes: Segurança de redes, referência rápida*. Tradução Ana Beatriz Tavares dos Santos Pereira, Daniela F. Lacerda Guazelli. Rio de Janeiro: Elsevier, 2003, 250p

IMAISUMI, R. P.; MARTINS, H. P. *Anomalias e segurança em redes computacionais: Uma abordagem prática com ataque DOS*, 2013. Disponível em: <http://www.fatecbauru.edu.br/ojs/index.php/CET/article/view/53/49c. Acesso em: 18 fev. 2014.

ISO 27002. *ABNT NBR ISO/IEC 27002. Tecnologia da Informação – Técnicas de segurança – Código de prática para gestão da segurança da informação*, 2005.

JCVIRTAL. Firewall – *Conceitos e principais tipos de firewall*, 2012. Disponível em: <http://www.jcvirtual.com.br/index.php/2011-12-29-12-54-04/130-firewall-conceito-e-principais-tipos>. Acesso em: 05 fev. 2014.

JORGE, H. V. N.; *Segurança da Informação e Crimes Cibernéticos*. 2011. Disponível em <http://www.crimesciberneticos.net/2011/01/man-in-middle-e-outras-tecnicas-em.html>. Acesso em: 21 jan. 2014.

KASPERSKY. *A utilização da análise heurística no Antivírus*, 2012. Disponível em < http:// support.kaspersky.com/6668/>. Acesso em: 24 fev. 2014.

KASPERSKY. *O que é um Ataque Man-in-the-Middle?,* 2013. Disponível em <http://blog. kaspersky.com.br /what-is-a-man-in-the-middle-attack/. Acesso em: 18 fev. 2014.

KEIZER, G. Vírus Duqu foi desenvolvido durante 4 anos, afirma Kaspersky, 2011. Disponível em: < http://idgnow.uol.com.br/seguranca/2011/11/14/virus-duqu-foidesenvolvido-durante-4-anos-afirma-kaspersky/>. Acesso em: 06 fev. 2014.

KRAUSE, M.; TIPTON, H. F. *Handbook of Information Security Management*. [s.l]: Auerbach Publications, 1999. 1.116p.

KUMAR, M. *New SSL/TLS atack for hijacking HTTPS sessions*, 2012. Disponível em: < http:// thehackernews.com/2012/09/crime-new-ssltls-attack-for-hijacking.html/>. Acesso em: 26 fev. 2014.

LAUREANO, M. A. P.; MORAES, P. E. S. *Segurança como Estratégia de Gestão da Informação. Revista Economia & Tecnologia*, 2005. p38-44. Disponível em <http://www.raposo.net.br/ images2/Segurança como estratégia de gestão da informação.pdf/>. Acesso em: 26 nov. 2013.

LEWIS, A. J. *Thresholds for Cyberwar. Center for Strategic and International Studies*, 2010.

LINHA DEFENSIVA. *O 'maior ataque cibernético' e outro grande exagero da imprensa*, 2013. Disponível em <http://www.linhadefensiva.org/2013/03/o-maior-ataque-cibernetico-e-outro-grande-exagero-da-imprensa/>. Acesso em: 18 fev. 2014.

MAIA, L. P. Analisando *Ataques do Tipo Distributed Denial of Service – DDoS*, 2003. Developers Magazine. n. 54, p. 26-27. Disponível em <http://www.linhadecodigo. com.br/artigo/303/ negacao-de-servico-implementacao-defesas-e-repercucoes.aspx Em: 31 de mar. de 2012.

MACEDO, D. *Conceitos de filtragem de pacotes e firewall*, 2012. Disponível em <http://www.diegomacedo.com.br/conceito-de-filtragem-de-pacotes-e-firewall/>. Acesso em: 28 nov. 2013.

MANDARINO J. R. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Cubzac, 2010.

MANDARINO, R.; CANONGIA, C. *Livro Verde Segurança Cibernética no Brasil*, 2010. Brasília: GSIPR/SE/DSIC. Disponível em:<http://dsic.planalto.gov.br/ documentos/publicacoes/1_Livro _Verde _SEG_ CIBER.pdf Acesso em: 28 nov. 2013.

MARTINEZ, F. L. Sistemas *Distribuidos de Denegación de Servicio*, 2000. Disponível em: <http:// panoramix.fi.upm.es/~flimon/ddos.pdf>. Acesso em: 22 jan.2014.

MCAFEE. *Gerenciamento de eventos e informações de segurança (SIEM),* 2014. Disponível em <http://www.mcafee.com/br/resources/reports/rp-siem-keeping-pace-big-security-data.pdf> Acesso em: 07 fev. 2014.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. *Hackers Expostos – Segredos e Soluções para redes*. 4 ed. São Paulo: Campus, 2003.

MCMILLAN, R. *Siemens: Stuxnet worm hit industrial systems,* 2010. Disponível em:<http://www. computerworld.com/s/article/print/9185419/Siemens_Stuxnet_ worm _hit_ industrial_systems?taxonomyName= Network+Security&taxonomyId=142>. Acesso em 07 fev.2014.

MICROSOFT. *Defesa em profundidade*, 2011. Disponível em <http://msdn.microsoft. com/ pt-br/library/ff716605.aspx#defesaprofund> Acesso em: 10 fev. 2014.

MICROSOFT. O *que é software antivírus?,* 2012. Disponível em <http://www. microsoft.com/pt-br/security/resources/antivirus-whatis.aspx> Acesso em: 24 fev. 2014.

MICROSOFT. *Definição das sete camadas do modelo OSI e explicação de suas funções*, 2013. Disponível em <http://support.microsoft.com/kb/103884/pt-br> Acesso em: 28 fev. 2014.

MILLES, E. *United Wisconsin website targeted by denial-of-service attack*, 2011. Disponível em: <http://dane101.com/current/2011/11/14/united_wisconsin_ website_targeted_by_denialofservice_ attack>. Acesso em: 15 jan. 2014.

MITNICK, K. D; SIMON W. L.. *A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação.* São Paulo: Pearson Education, 2003.

MORAES. *Múltiplas camadas de defesa: A complementaridade do Firewall e do IPS*, 2012. Disponível em: http://alexandremspmoraes.wordpress.com/2012/07/03/ multiplas-camadas-de-defesa-a-complementaridade-do-firewall-e-do-ips/>. Acesso em: 04 fev. 2014.

MUSEU. *O que é HD?,* 2004. Disponível em: http://www.museudocomputador. com.br/enciclohd.php. Acesso em: 15 jan. 2014.

MORINOTO, C. E.; *Bloqueando ataques de Syn flood*. 2010. Disponível em <http://www.hardware. com.br/dicas/syncookies.html>. Acesso em: 15 jan. 2014.

MORINOTO, C. E. *Gateway*, 2005. Disponível em < http://www.hardware.com.br/ termos/gateway>. Acesso em: 21 jan. 2014.

NETWORK BOX. *Anti-DDoS (Distributed Denial of Service),* 2011. Disponível em <http://www. network-box.com/anti-ddos> Acesso em: 12 fev. 2014.

NEWMAN, J. Saiba *mais sobre o vírus "Flame",* 2012a. Disponível em: <http://pcworld. uol.com.br/noticias/2012/05/31/saiba-mais-sobre-o-virus-201cflame 201d/>. Acesso em: 05 dez. 2013.

NEWMAN, J. *Entenda tudo sobre o 'supervírus' Flame*, 2012b. Disponível em: <http://idgnow.uol.com.br/internet/2012/05/31/entenda-tudo-sobre-o-supervirus-flame/>. Acesso em: 17 dez. 2013.

NORTHCUTT, S. et al*. Inside Network Perimeter Security*. 2ed. [s.l.]:Sans Institute, 2005, p.55

OLIVEIRA, L. H. A. *Cyberwar: Novas Fronteiras Da Guerra,* 2011. Monografia - Universidade de Brasília, 2011. Disponível em: <http://bdm.bce.unb.br/bitstream/ 10483/1991/1/2011_ LuisHenriqueAlmeidadeOliveira.pdf/>. Acesso em: 04 jan. 2014.

OWASP. *OWASP Best Practices: Use of Web Application Firewalls*, 2008. Disponível em: <https://www.owasp.org/index.php/Category:OWASP_Best_ Practices:_Use_of_ Web_ Application_Firewalls/>. Acesso em: 04 fev. 2014.

OWASP. *SQL Injection*, 2013. Disponível em: < https://www.owasp.org/ index.php/ SQL_Injection/>. Acesso em: 05 fev. 2014.

OWASP. *Web aplication firewall*, 2011. Disponível em: < https://www.owasp.org/index.php/Session_ hijacking_attack>. Acesso em: 04 fev. 2014.

OWASP. *Session hijacking attack*, 2014. Disponível em: <https://www.owasp.org/ index.php/ Web_Application_Firewall/>. Acesso em: 04 fev. 2014.

PARKS, R. C.; DUGGAN, D. P. *Principles of Cyber-warfare Proceedings of the IEEE Workshop on Information Assurance.* Trabalho apresentado no Seminário de

Segurança da Informação da Academia Militar dos Estados Unidos da América, 2001. p122 – 125.

PASQUALE, A. D. *ArpON 2.7 Released!,* 2011. Disponível em: <http://arpon. sourceforge.net http>. Acesso em: 27 jan. 2014.

PEIXOTO, M. C. P. *Engenharia Social e Segurança da Informação na Gestão Corporativa*. Rio de Janeiro: Brasport, 2006.

PIRES, A. S. O kernel *do Linux: A definição, importância e funcionalidades*, 2007. Disponível em: <http://www.vivaolinux.com.br/artigo/O-kernel-do-Linux-A-definicao-importancia-e-funcionalidades?pagina=2>. Acesso em: 27 jan. 2014.

RAFAEL, G. C. *Engenharia Social: as técnicas de ataques mais utilizadas*, 2013. Disponível em: <http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 13 jan. 2014.

REYES, M. A. *Hackers atacam sites via Defacement! veja o que é e como se proteger*, 2010. Disponível em: <http://webinhost.com.br/blog/blog-dicas/o-que-se-entende-por-defacement/>. Acesso em: 27 jan. 2014.

REQUEST FOR COMMENTS. *RFC 768: User Datagram Protocol.* Ago. 1980. 2p. Disponível em <http://tools.ietf.org/html/rfc768>. Acesso em: 20 jan. 2014.

REQUEST FOR COMMENTS. *RFC 792: Internet Control Message Protocol.* Set. 1981. 18p. Disponível em <http://tools.ietf.org/html/rfc792>. Acesso em: 20 jan. 2014.

REQUEST FOR COMMENTS. RFC *4987: TCP SYN Flooding Atack.* Ago. 2007. 1p. Disponível em < http://tools.ietf.org/html/rfc4987>. Acesso em: 20 jan. 2014.

REQUEST FOR COMMENTS. RFC *6071: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*. fev. 2011. 53p. Disponível em < http://tools.ietf.org/html/rfc6071>. Acesso em: 04 fev. 2014.

ROHR, A. *Agobot*, 2004. Disponível em: <http://www.linhadefensiva.org/2004/10/ agobot/>. Acesso em: 25 de jan. 2014.

RSNAKE, *Slowloris.pl*. Disponível em: <http://ha.ckers.org/slowloris/slowloris.pl>. Acesso em: 20 jan. 2014.

RUFINO, N.M.O. *Segurança em redes sem fio*. 3ed. São Paulo:Novatec, 2011.

SALVATORE, R. *Implementando uma defesa em profundidade para sua rede,* 2012. Disponível em: <http://cassioaramos.blogspot.com.br/2012/03/artigo-sobre-defesa-em-profundidade.html>. Acesso em: 15 fev. 2014.

SANCHES, F. *O que é GRC*?, 2008. Disponível em: <http://grcnews.blogspot. com.br/2008/06/o-que-grc.html>. Acesso em: 15 fev. 2014.

SANGER, D. E. Obama *Order Sped Up Wave of Cyberattacks Against Iran*, 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave -of-cyberattacks-against-iran.html?_r=4&ref=technology>. Acesso em: 11 dez. 2013.

SAUVAGE, S. *O que são SSL, SSH, HTTPS?,* 2014. Disponível em: <http://pt.kioskea.net/faq/9943-o-que-sao-ssl-ssh-https>. Acesso em: 21 fev. 2014.

SCHLEMER, E. *Iptables protege contra SYN FLOOD*?, 2007. Disponível em:<http://www.vivaolinux.com.br/artigo/Iptables-protege-contra-SYN-FLOOD/>. Acesso em: 15 jan. 2014

SCHWARTAU, W. *Information Warfare*. 2ed. [s.l.]: Thunders Mouth Press, 1994.

SHEETER, L. *Estônia acusa Rússia de "ataque cibernético" ao país,* 2007. Disponível em:<http://www.bbc.co.uk/portuguese/reporterbbc/story/2007/05/070517 _estoniaataquesinter netrw.shtml>. Acesso em: 13 dez. 2013

SEGINFO. *Ataques DRDoS aumentam 265% comparado ao mesmo período de 2012, de acordo com pesquisa feita pela Prolexic*, 2013. Disponível em: <http://www.seginfo.com.br/ ataques- drdos- aumentam-265- comparado -ao-mesmo-periodo-de-2012-de-acordo-com-pesquisa-feita-pela-prolexic/>. Acesso em: 05 fev. 2014.

SILVA, L. G. *Stuxnet e a nova geração de ameaças cibernéticas*. 2011a. Disponível em: <http://www.tiespecialistas.com.br/2011/05/stuxnet-e-a-nova-geracao-de-ameacas-ciberneticas/>. Acesso em: 11 dez. 2013.

SILVA, A. *Segurança em Redes e Telecomunicação – Parte 2,* 2011b. Disponível em: <http://hercules-now.com/2011/05/23/seguranca-em-redes-e-telecomunicacao-parte-2//>. Acesso em: 05 fev. 2014.

SOLHA, L. E. V. A. at al. *Tudo que você precisa saber sobre os ataques DDoS*, 2004. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: 13 dez. 2013

SYMANTEC. *Relatório de Ameaças à Segurança na Internet (ISTR),* 2012a. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_ resources/b-istr_main_report_v18_2012_ 21291018.en-us.pdf>. Acesso em: 11 dez. 2013.

SYMANTEC. *Glosálio Symantec -Smurf DoS attack (ataque de DoS Smurf),* 2012b. Disponível em: <http://www.symantec.com/pt/br/security_response/glossary/define. jsp?letter=s&word=smurf-dos-attack>. Acessdo em: 31 de marco de 2012.

TOMICKI, L. *Ping Flooding,* 2010. Disponível em: <http://tomicki.net/ping. flooding.php>.Acesso em: 20 jan. 2014.

UFES. *O que significam as siglas IPS e IDS, no contexto de redes de computadores?,* 2010. Disponível em: <http://www.npd.ufes.br/node/87>. Acesso em: 04 fev. 2014.

UFES*. Blacklist x Whitelist*, 2014. Disponível em: <http://www.npd.ufes.br/ node/85#10>. Acesso em: 11 fev. 2014.

ULBRICH, H. C. *Universidade H4CK3R*, 2009. 2ed. São Paulo: Digerati Books. p.337.

UNISYS. *Security Operations Center*, 2014. Disponível em: <http://www.unisys.com/ unisys/countrysite/aos/index.jsp?cid=400008&id= 2700046>. Acesso em: 28 jan. 2014.

VAZ, H. *Introdução à segurança da Informação*, [201-?]. Disponível em: < http://pt.slideshare.net/higsonvaz/livro-cap01>.Acesso em: 18 fev. 2014.

VERLY, A. C. *Perigo na rede: sites do governo sofrem ataques de hackers,* 2011. Disponível em <http://www.conexaoprofessor.rj.gov.br/atualidade_detalhe.asp? Edite CodigoDaPagina=7271&Pagina=1/>. Acesso em: 21 jan. 2014.

VIANNA, N. *Defesa Cibernética na visão da MB*, 2012. Disponível em: <http://www. eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/viewFil e/24/38>. Acesso em: 11 dez. 2013.

VIEIRA, L. *XSS – Cross Site Scripting*, 2008. Disponível em: < http://www http://imasters.com.br/artigo/9879/seguranca/xss-cross-site-scripting/>. Acesso em: 05 fev. 2014.

VIEIRA, L. *ARP Poisoning: compreenda os princípios e defenda-se*, 2009. Disponível em: <http://www.vivaolinux.com.br/artigo/ARP-Poisoning-compreenda-os-principios-e-defendase. Acesso em: 22 fev. 2014.

TÁCIO, P. *Ferramentas para DoS/DDos T50,* 2010. Disponível em <http://www.mundodoshackers.com.br/ferramenta-para-dosddos-t50/>. Acesso em: 23 jan. 2014.

TANENBAUM, Andrew S. *Redes de Computadores*. Tradução Vandenberg D. de Souza. 4.ed. Rio de Janeiro: Elsevier, 2003.

TCP/IP GUIDE. *The TCP/IP Guide Versão 3.0*, 2005. Disponível em <http://www.tcpipguide.com/ free/ t_TCPConnectionEstablishment ProcessTheThree WayHandsh-3.htm>. Acesso em: 15 jan. 2014.